대한민국 특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2001년 제 45856 호
Application Number PATENT-2001-0045856

출 원 년 월 일 : 2001년 07월 30일
Date of Application JUL 30, 2001

출 원 인 : 주식회사 마크애니
Applicant(s) MARKANY INC.

2001 년 12 월 05 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2001.07.30

【국제특허분류】 G06F

【발명의 명칭】 디지털 정보 보안 방법 및 그 시스템

【발명의 영문명칭】 METHOD OF PROTECTING DIGITAL INFORMATION AND SYSTEM THEREOF

【출원인】

【명칭】 주식회사 마크애니

【출원인코드】 1-1999-026375-7

【대리인】

【성명】 권혁록

【대리인코드】 9-1998-000115-1

【포괄위임등록번호】 2001-032418-2

【발명자】

【성명의 국문표기】 최종욱

【성명의 영문표기】 CHOI,Jong Uk

【주민등록번호】 520303-1812414

【우편번호】 142-090

【주소】 서울특별시 강북구 우이동 1 성원 아파트 2-1301

【국적】 KR

【발명자】

【성명의 국문표기】 이원하

【성명의 영문표기】 LEE,Won Ha

【주민등록번호】 730205-1148415

【우편번호】 130-083

【주소】 서울특별시 동대문구 이문3동 64번지 쌍용아파트 106동 1704호

【국적】 KR

【발명자】

【성명의 국문표기】 조정석

【성명의 영문표기】 CHO,Jung Seok

【주민등록번호】 730217-1056911
【우편번호】 423-060
【주소】 경기도 광명시 하안동 하안 주공아파트 401-410
【국적】 KR
【발명자】
【성명의 국문표기】 장완호
【성명의 영문표기】 JANG,Wan Ho
【주민등록번호】 670706-1000810
【우편번호】 427-050
【주소】 경기도 과천시 부림동 주공아파트 808-1407호
【국적】 KR
【발명자】
【성명의 국문표기】 서지선
【성명의 영문표기】 SEO,Ji Sun
【주민등록번호】 750208-2408026
【우편번호】 120-132
【주소】 서울특별시 서대문구 북가좌2동 304-1
【국적】 KR
【조기공개】 신청
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인
권혁록 (인)
【수수료】
【기본출원료】 20 면 29,000 원
【가산출원료】 48 면 48,000 원
【우선권주장료】 0 건 0 원
【심사청구료】 0 항 0 원
【합계】 77,000 원
【감면사유】 중소기업
【감면후 수수료】 38,500 원
【첨부서류】 1. 요약서·명세서(도면)_1통 2.중소기업법시행령 제2조에의한 중소기업에 해당함을 증명하는 서류 _1통 3.위임장_1통

【요약서】

【요약】

본 발명은 디지털 정보 보안을 위하여 사용자 단말의 시스템 고유 정보를 이용하여 해당 사용자의 고유 키를 생성하는 사용자 애플리케이션 툴과, 사용자 애플리케이션 툴에서 생성한 사용자 고유 키를 제공받아 이를 데이터 저장부에 해당 사용자 정보의 일부로써 저장토록 하며, 사용자 인증시에 저장된 사용자 고유 키와 현재 인증하는 사용자의 사용자 애플리케이션 툴에서 제공되는 사용자 고유 키의 일치 여부를 비교하는 사용자 관리 툴을 구성하며, 서버에서 사용자의 접속시에 해당 사용자 단말의 시스템 고유 정보를 이용하여 생성된 사용자 고유 키를 읽어들이고, 읽어들인 사용자 고유 키와 미리 저장된 현재 접속한 사용자에 대한 사용자 정보에 포함된 사용자 고유 키를 비교하여 접속한 사용자의 적합 여부를 인증하고, 인증한 사용자의 파일 업로드시에 해당 파일을 미리 설정된 암호화 키를 이용한 암호화 방식으로 암호화하여 디지털 정보로써 저장하며, 인증한 사용자의 디지털 정보의 다운로드 요청시에 해당 디지털 정보를 상기 사용자 정보에 포함된 사용자 고유 키를 이용하여 암호화하여 다운로드 한다.

【대표도】

도 2

【색인어】

디지털 정보, 보안, 암호, DRM

【명세서】

【발명의 명칭】

디지털 정보 보안 방법 및 그 시스템{METHOD OF PROTECTING DIGITAL INFORMATION AND SYSTEM THEREOF}

【도면의 간단한 설명】

도 1은 본 발명의 일 실시예에 따른 디지털 정보 보안 시스템의 개략적인 전체 블록 구성도

도 2는 도 1 중 기업정보서버 및 터미널의 블록 구성도

도 3은 본 발명의 일 실시예에 따른 기업정보서버에서의 사용자 등록 과정의 동작 흐름도

도 4는 본 발명의 일 실시예에 따른 기업정보서버에서의 사용자로부터의 기업문서 업로드 과정의 동작 흐름도

도 5는 본 발명의 일 실시예에 따른 기업정보서버에서의 사용자로 기업문서 다운로드 과정의 동작 흐름도

도 6은 본 발명의 다른 실시예에 따른 디지털 정보 보안 시스템의 개략적인 전체 블록 구성도

도 7은 도 6 중 문서키관리 서비스 모듈의 동작을 설명하기 위한 도면

도 8은 도 6중 문서관리 서비스 게이트웨이의 동작을 설명하기 위한 도면

도 9는 도 6중 문서배포 서비스 모듈의 동작을 설명하기 위한 도면

도 10은 본 발명의 일 실시예에 따른 디지털 정보 보안 시스템에서 사용자 관리 툴의 운영자 인터페이스 화면의 예시도

도 11a는 도 10의 관리 툴 인터페이스 화면 중 해당 부서의 모든 사람에게 모든 권한을 부여하기 위한 화면의 예시도

도 11b는 도 10의 관리 툴 인터페이스 화면 중 해당 부서의 모든 사람에게 모든 권한이 부여된 상태를 나타내는 화면의 예시도

도 12a는 도 10의 관리 툴 인터페이스 화면 중 새로운 부서를 추가하기 위한 화면의 예시도

도 12b는 도 10의 관리 툴 인터페이스 화면 중 새로운 부서가 추가된 상태를 나타낸 화면의 예시도

도 13a는 도 10의 관리 툴 인터페이스 화면 중 특정 사용자의 사용자 정보의 변경을 위한 화면의 일 예시도

도 13b는 도 10의 관리 툴 인터페이스 화면 중 특정 사용자의 사용자 정보의 변경을 위한 화면의 다른 예시도

도 14a는 본 발명의 일 실시예에 따른 문서 저장 권한이 없는 사용자가 해당 문서의 저장을 시도한 경우의 출력 화면의 예시도

도 14b는 본 발명의 일 실시예에 따른 문서 프린트 권하니 없는 사용자가 해당 문서의 프린트를 시도한 경우의 출력 화면의 예시도

도 15는 본 발명의 일 실시예에 따른 문서 뷰어를 이용한 문서를 일반 문서 제작 프로그램을 통해 오픈한 경우의 화면 예시도.

도 16은 본 발명의 일 실시예에 따른 다운로드 받은 파일을 복사 및 다른 시스템에서 오픈한 경우의 출력 화면의 예시도

도 17a, ~ 17e는 각각 본 발명의 일 실시예에 따른 문서 뷰어를 이용하여 "POWERPOINT' 파일, " MS-WORD' 파일, 'EXCEL' 파일, "훈민정음" 파일 및 " AutoCAD' 파일을 오픈한 경우의 출력 화면의 예시도

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<22> 본 발명은 기업 및 기관의 공용 컴퓨터에 저장된 디지털 정보를 유, 무선의 통신상이나 디스켓 등의 저장매체를 통하여 복사하여 이를 외부로 유출하는 것을 보안하는 방법 및 그 시스템에 관한 것으로써, 특히 기업 및 기관에서 공유되고 있는 디지털 문서나 프로그램과 같은 디지털 정보에 대하여 내부 사용자(또는 외부 사용자)가 이를 불법적으로 사용하는 것을 방지하기 위한 방법 및 시스템에 관한 것이다.

<23> 최근, 각종 문서와 데이터 등과 같은 정보들이 컴퓨터에 의해 디지털화되고, 인터넷이나 이메일 및 디지털 저장매체들이 발달함에 따라, 원하는 자료(이하 디지털 정보라 총칭함)를 보다 신속하고 용이하게 얻을 수 있는 기회가 주어지고 있다.

<24> 그런데 이러한 디지털 정보의 특성상 원본과 동일한 복사본 혹은 변형본을 쉽게 만들어 낼 수 있을 뿐 아니라, 손쉽게 배포할 수 있기 때문에 이러한 불법적인 복사 및 배포 등으로 인하여 기업이나 기관의 기밀이 누출을 통해 기업이나 국가 경쟁력의 약화까지 초래할 수 있는 문제점이 대두되고 있다.

<25> 특히, 최근에 기업 내에서의 LAN(Local Area Network)이나 KMS(Knowledge Management System) 구축이 급격히 진행됨에 따라 기업 내의 정보나 자료가 간단히 왕래되고 있으므로, 이에 따른 디지털 정보의 접근의 용이성으로 인하여 기업이나 기관의 정보노출의 가능성이 더더욱 증대되고 있는 실정이다. 실제로 해당 기업의 직원들이 다른 기업으로 이직, 혹은 퇴직하면서 기업 내의 기밀을 불법적으로 유출하는 일도 아울러 증가하고 있다.

<26> 따라서 이러한 디지털 정보의 보호기술에 대한 요구가 급증하고 있으며, 불법적인 배포 및 사용을 막기 위한 기술과 서비스분야에 대한 다양한 기술이 개발되고 있다. 이러한 기술로는 시스템 로그인의 관리와 시스템의 불법 접근을 봉쇄하기 위한 시스템 관리기법으로 방화벽 설치 기술과, 디지털 문서를 보호하고 보안 및 관리하는 디지털 저작권 관리(Digital Rights Management: 이하 DRM이라 함) 기술 및 전자메일의 사용자 제한 기술 등을 들 수 있다.

<27> 시스템 보안, 네트워크 보안, 시설보안 등을 위한 방화벽 설치 기술은 주로 외부로부터의 불법적인 침입을 방지하기 위한 기술로써, 주로 기업이나 기관의 사용자를 관리하기보다는 외부에서의 침입방지에 그 목적을 두고 있기 때문에 기업 혹은 기관 내에서의 불법적인 침입이나 행위에 대해서는 제대로 역할을 수행하지 못하는 문제점 있다.

<28> DRM 기술은 멀티미디어 정보의 불법유통과 복제를 방지하고, 적법한 사용자만이 정보를 사용할 수 있도록 사용자를 관리하며, 결재 등과 같은 과금 서비스를 통해서 멀티미디어 정보의 저작권을 관리하는 기술이다. 이러한 DRM 기술은 현재 시장에서 디지털 정보의 저작권을 보호하고 관리할 수 있는 현실적인 솔루션으로 받아들여지고 있으나, 현재의 DRM 시스템은 그 구조와 시스템이 매우 복잡하고 비대하여 실제로 사용자가 이를 적용하여 서비스를 실시하기는 용이하지 않는 문제점이 있다.

<29> 특히, 일반 사용자들이 정보를 실제로 구매하여 이를 재생 활용함에 있어 이용되는 인증키(key)의 관리문제가 전적으로 DRM 서버 제공자 측에서 운영되는 경우가 많고, 실제 정보도 서버등록자에게 전송하여 이를 등록, 암호화 한 후에 이를 다시 받아서 운영하는 경우가 많다. 이에 따라 일반 기업이나 기관 등에서 사용시에는 시스템의 구축 측면, 실제 정보의 관리 측면에서 정보를 서버등록자에게 보내고 다시 받아야 하는 이중 작업의 불편함이 있으며. 전송경로가 복잡하게 되어 중간에서 정보가 외부로 누출될 수 있는 가능성이 높아지게 된다.

<30> 더욱이 이러한 DRM 기술의 경우에, 정보를 둘러싸고 있는 암호화가 풀렸을 경우 소스 정보(source contents)가 쉽게 유통될 수 있는 우려가 있다. 또한 상기 기존의 DRM을 이용한 정보 보호에 있어서는 정보 제공자와 정보 사용자의 루트가 일방적인 루트를 이루고 있어서 정보 유통체계에 있어 상호 의견교환을 통한 유통체계의 원활한 소통이 어렵다. 이러한 DRM 기술을 기업이나 정부 등의 문서보안을 위해 적용하는 경우 보안을 위한 대상문서를 모두 서버등록자에게 보내

어 암호화 한 후에 다시 이를 받아서 배포해야 하는 불편함이 있기 때문에 상업적인 목적의 정보 이외에는 적용하기가 어렵다는 단점도 아울러 가지고 있다.

<31> 한편, 전자메일의 관리를 통한 문서 보안의 경우는 전자메일의 첨부파일의 용량을 제한하거나 TCP/IP(Transmission Control Protocol/Internet Protocol)의 트래픽에 대한 통제, 또는 모니터링을 통한 통제를 통하여 리스트를 작성하여 리포팅하거나 경보를 통해 주의를 환기시키거나, 또는 사용자의 감시 등을 수행하는 기술이다. 그런데 이메일의 관리를 통한 문서보안은 자칫하면 기업이나 기관의 개개인 정보를 감시한다는 점에서 개인의 자유를 침해한다는 문제점을 안고 있다. 또한 최근에는 이메일 이외에도 월드 와이드 웹(World wide web: WWW)이나 FTP(File Transfer Protocol) 등을 통해 파일 전송이 가능하고 또한 플로피 디스크, "Zip" 디스크 "Jazz" 디스크, 콤팩트디스크(compact disc)와 같은 대용량의 저장매체의 발달로 이를 통해 정보가 누출되는 경로를 차단할 수가 없다는 문제점을 안고 있다. 최근에는 PDA(Personal Digital Assistant)와 같은 무선을 통해 자료나 데이터, 프로그램을 전송할 수 있기 때문에 이메일의 통제를 통한 문서보안은 한계성을 드러내고 있다.

【발명이 이루고자 하는 기술적 과제】

<32> 따라서 본 발명의 목적은 기업이나 기관의 중요 문서나 데이터, 프로그램 등의 디지털 정보 보안을 위하여 내부의 불법적인 사용을 방지할 수 있는 디지털 정보 보안 방법 및 그 시스템을 제공함에 있다.

<33> 본 발명의 다른 목적은 기업이나 기관의 중요 문서나 데이터, 프로그램 등의 디지털 정보가 불법적으로 누출되었더라도 불법적인 사용을 방지할 수 있는 디지털 정보 보안 방법 및 그 시스템을 제공함에 있다.

<34> 상기한 목적을 달성하기 위하여 본 발명의 일 측면은 디지털 정보 보안 시스템에 있어서, 사용자 단말에 설치되며, 사용자 단말의 시스템 고유 정보를 이용하여 해당 사용자의 고유 키를 생성하는 사용자 애플리케이션 툴과, 사용자 정보 및 디지털 정보를 저장하는 데이터 저장부와, 서버에 설치되며, 사용자 애플리케이션 툴에서 생성한 사용자 고유 키를 제공받아 이를 데이터 저장부에 해당 사용자 정보의 일부로써 저장토록 하며, 사용자 인증시에 저장된 사용자 고유 키와 현재 인증하는 사용자의 사용자 애플리케이션 툴에서 제공되는 사용자 고유 키의 일치 여부를 비교하는 사용자 관리 툴을 포함하여 구성함을 특징으로 한다.

<35> 본 발명의 다른 측면은 디지털 정보 보안 방법에 있어서, 서버에서 사용자의 접속시에 해당 사용자 단말의 시스템 고유 정보를 이용하여 생성된 사용자 고유 키를 읽어들이는 과정과, 읽어들인 사용자 고유 키와 미리 저장된 현재 접속한 사용자에 대한 사용자 정보에 포함된 사용자 고유 키를 비교하여 접속한 사용자의 적합 여부를 인증하는 과정과, 인증한 사용자의 파일 업로드시에 해당 파일을 미리 설정된 암호화 키를 이용한 암호화 방식으로 암호화하여 디지털 정보로써 저장하는 과정과, 인증한 사용자의 디지털 정보의 다운로드 요청시에 해당 디

지털 정보를 상기 사용자 정보에 포함된 사용자 고유 키를 이용하여 암호화하여 다운로드 하는 과정을 포함하여 구성함을 특징으로 한다.

【발명의 구성 및 작용】

<36> 이하 본 발명에 따른 바람직한 실시예를 첨부한 도면을 참조하여 상세히 설명한다. 하기 설명에서는 구체적인 구성 소자 등과 같은 특정 사항들이 나타나고 있는데 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐 이러한 특정 사항들이 본 발명의 범위 내에서 소정의 변형이나 혹은 변경이 이루어질 수 있음은 이 기술분야에서 통상의 지식을 가진 자에게는 자명하다 할 것이다.

<37> 본 발명은 보안되어야 할 디지털 정보(하기 설명에서는 기업문서라 칭함)가 제작되어 기업내 정보로서의 가치를 가지게 되는 순간부터 네트워크를 통해 또는 오프라인 상의 어떠한 경로를 거쳐 다양한 사용자들이 이용하게 되는 과정에서부터 해당 기업문서가 폐기되는 순간까지의 모든 생성, 배포 및, 폐기의 전 과정에 걸친 보안 방법 및 장치를 제시한다. 본 발명은 기업문서를 보호하면서 정당한 방법으로 사용자들에게 그 사용 권리를 허가하여 함부로 정보를 도용, 위조, 변조할 수 없도록 하는 등의 모든 관리 체계를 제안한다.

<38> 도 1은 본 발명의 일 실시예에 다른 디지털 정보 보안 시스템의 개략적인 전체 블록 구성도이다. 도 1을 참조하면, 기업정보 서버(10)는 내부망을 통해 개인용 컴퓨터와 같은 다수의 터미널(14)과 연결되며 또한 데이터 통신망인 PSDN(Packet Switched Data Network)(20)을 통해 원격지의 사용자들과 접속될 수

있으며, 본 발명에 따라 기업 정보를 제공하거나 또는 소정 회사에서 자료를 제공하는 시스템이다.

<39> 기업정보 서버(10)는 운영자 컴퓨터(12)와 접속되며, 운영자 컴퓨터(12)로부터 수신되는 명령에 의해 본 발명에 따른 디지털 정보 보안 동작의 다양한 세부 사항들이 설정될 수 있다. 서버 관리자는 이러한 운영자 컴퓨터(12)를 통해 기업정보 서버(10)를 관리하며 동작을 제어하게 된다.

<40> PSDN(20)을 통해 연결되는 원격지의 사용자는 개인용 컴퓨터(22)를 이용하여 상 상기 기업정보 서버(10)에 접속할 수 있다. 이러한 사용자 컴퓨터(22)는 PSDN(20)을 통해 기업정보 서버(10)와 연결되어 본 발명에 따라 암호화된 기업정보를 제공받을 수 있다. 이와 다른 방법으로 상기 사용자 컴퓨터(22)는 근거리 통신망(LAN)을 이용하거나 원거리 통신망(WAN) 등을 이용하여 기업정보 서버(10)와 연결될 수도 있으며, 이는 PSDN(10)에 포함되는 것으로 설명한다.

<41> 상기와 같이 내부망 또는 PSDN(20)을 통해 본 발명의 기업정보 서버(10)에 접속하여 암호화된 기업정보를 제공받거나 또는 기업정보를 제공하는 터미널(14) 또는 사용자 컴퓨터(22)에는 본 발명의 특징에 따라 디지털 정보 보안을 위한 애플리케이션 툴이 설치되며, 상기 기업정보 서버(10)에는 이러한 터미널(14) 또는 사용자 컴퓨터(22)를 이용하는 사용자를 관리하며, 제공되는(또는 제공받는) 기업정보를 보안하며 관리하기 위한 관리 툴 및 각종 데이터 저장용 데이터베이스가 구축된다. 이를 도 2를 참조하여 보다 상세히 설명하기로 한다.

<42> 도 2는 도 1 중 기업정보 서버(10) 및 이에 접속된 터미널(14)의 블록 구성도이다. 기업정보 서버(10)는 크게 네트워크 인터페이스(110)와, 데이터 유통 경

로(120)와, 서버 제어부(130)와, 데이터 저장부(140)와, 이력 관리부(150) 및 운영자 컴퓨터 인터페이스부(160)로 구성된다.

<43> 네트워크 인터페이스(110)는 PSDN(20) 및 내부망과 연결되어 내부 터미널(14) 및 사용자 컴퓨터(22)로부터 수신되는 데이터를 데이터 유통 경로(120)로 전달하고, 데이터 유통 경로(120)로부터 입력된 데이터를 PSDN(20) 또는 내부망을 통해 각 해당 단말로 전달한다.

<44> 데이터 유통 경로(120)는 본 발명의 시스템 구성에 따라 다르게 구성할 수 있다. 예를 들어 하나의 시스템으로 구성하는 경우 각 기능부간 데이터를 전달하기 위한 버스로 구성할 수 있다. 다른 예로 각 기능부가 독립적인 하나의 시스템으로 구성되는 경우 근거리 통신망(LAN) 등을 이용하여 연결할 수도 있다. 또한 상기 몇 개의 기능부들이 독립적인 시스템을 이루며 그 내부에서 각기 연결되는 경우 독립적인 시스템들은 근거리 통신망으로 연결하고, 내부에서 연결되는 장치들은 버스로 구성할 수도 있다. 이와 같이 상기 데이터 유통 경로(120)는 데이터를 전달하기 위한 다양한 방식을 사용하여 구성할 수 있다.

<45> 기업정보 서버(10)를 총괄적으로 제어하는 서버 제어부(130)는 서버에 초기 접속 시의 화면 정보 및 공개가 가능한 자료들을 표시하는 각종 처리를 수행한다. 또한 게시판 및 일반 운영자 메일 정보를 제공하는 등의 각종 정보의 보안이 필요하지 않은 데이터들을 처리하기 위한 정보들을 제공한다. 또한 본 발명의 특징에 따라 문서의 암호화 및 사용자의 기업 문서 접근이 요구되는 경우 사용자 인증 및 기업 문서 다운로드/업로드 등에 대한 각종 동작을 제어한다. 이러한 서

버 제어부(130)에는 암호화키 및 사용자 고유 키를 관리하는 사용자 관리 툴(132)이 내장된다.

<46> 데이터 저장부(140)는 인터페이스부(141), 규칙설정부(142), 암호부(143), 결합부(144), 암호문서 DB(145), 사용자정보 DB(146), 기업문서정보 DB(146), 기업문서 DB(148), 및 규칙 DB(149)를 포함하여 구성된다.

<47> 인터페이스부(141)는 외부로부터 데이터 유통 경로(120)를 통해 입력되는 데이터의 목적지에 따라 각 내부 기능부 또는 데이터 베이스들로 제공하거나 또는 각종 데이터 베이스의 데이터를 읽어와 이를 외부 다른 기능부로 전달토록 데이터 유통 경로(120)로 출력한다. 규칙설정부(142)는 규칙 DB(149)에 기록 및 저장된 각종 규칙 설정 사항에 따라 사용자 및 문서에 대한 제반 사항이나 규칙들을 설정한다. 기업문서 DB(148)는 기업문서를 저장하며, 기업문서정보 DB(147)는 기업문서 정보를 저장하며, 사용자정보 DB(146)은 사용자 고유키 등을 포함한 사용자 정보를 저장한다. 암호부(143)는 암호화 키를 통해 상기 기업문서 DB(148), 기업문서정보 DB(147) 및 사용자정보 DB(146)에 저장되는 각종 정보를 암호화한다. 결합부(144)는 기업문서와, 사용자 고유키, 암호화키, 규칙 등을 결합하여 암호화하여 이를 암호문서 DB(145)에 저장한다. 상기에서 암호문서 DB(145), 사용자정보 DB(146), 기업문서정보 DB(146), 기업문서 DB(148), 및 규칙 DB(149) 등은 논리적으로는 분리되어 있으나, 물리적으로는 하나의 데이터베이스에 구축될 수 있다.

<48> 이력 관리부(150)는 이력 관리 장치(151)와 사용 이력 메모리(152)로 구분할 수 있다. 상기 이력 관리 장치(151)는 네트워크 인터페이스(110)로부터 제공

되는 정보의 열람 이력에 따른 정보가 수신되는 경우 이를 각 정보들로 구분하고 이를 사용 이력 메모리(152)에 저장한다. 이러한 이력 정보는 보안 등급이 높은 정보일수록 더욱 필요한 조건이 된다.

<49> 한편, 기업문서를 작성하고 사용하는 사용자부(도 1의 실시예에서는 터미널(14))에는 사용자 애플리케이션 툴(214)이 설치되는데, 이러한 사용자 애플리케이션 툴(214)은 자신이 설치된 사용자의 시스템의 ID 등을 이용하여 사용자 고유 키를 생성하고 이를 기업정보 서버(10)로 전송하게 된다.

<50> 즉, 사용자는 사용자 등록을 통하여 상기 기업정보 서버(10)에서 사용자 애플리케이션 툴(214)을 다운로드받아서 설치하게 되며, 사용자 애플리케이션 툴(214)은 자신이 설치된 고유 시스템 ID를 이용하여 사용자 고유 키를 생성하고 이를 기업정보 서버(10)로 전송하여 사용자 등록을 행하도록 한다.

<51> 상기 과정에서 발생하는 디지털 정보의 사용에 대한 인증과 관련하여, 사용자 애플리케이션 툴(214)은 각종 사용 가능한 조건 및 사용자 고유 키를 사용자 관리 툴(132)에 제공하고, 이 조건에 대한 자료 또는 신호를 전송한다. 이에 따라 사용자 관리 툴(132)은 사용자의 고유 키 정보를 사용자 애플리케이션 툴(214)로부터 전송받아 규칙설정부(142)를 통해 기업문서 파일을 제어하기 위한 각종 규칙들을 규칙 DB(149)로부터 받아 규칙을 설정한다. 사용자의 고유 키에 관한 정보는 사용자 정보 DB부(146)에 저장된다.

<52> 사용자(10)가 업로드한 기업문서는 기업문서 DB(148)에 저장되고 이 문서는 규칙설정부(142)에서 설정된 기업문서의 설정범위와 사용자 정보 등과 함께 결합부(144)에서 사용자 고유 키와 기업문서 암호화 키와 함께 결합된다. 이렇게 암

호화된 기업문서는 LAN이나 오프라인 경로를 통하여 또는 인터넷을 통하여 웹(Web) 상에서 사용자 암호입력 및 사용자 인증 절차를 거쳐 다시 사용자 애플리케이션 툴(214)로 제공되며 사용자를 이를 통해 기업정보를 받거나 열람할 수 있게 된다.

<53> 상기에서 설명한 사용자 애플리케이션 툴(214)과 사용자 관리 툴(132)은 본건 출원인에 선출원된 특허 출원번호 제2001-23562호의 CCR(Contents control Region: 컨텐츠 접근 제어부) CTS(Contents turn key system: 통합적인 컨텐츠 보호 및 관리 시스템)에 보다 상세히 개시된다.

<54> 한편, 상기 사용자 애플리케이션 툴(214)에서 사용자의 고유 키 생성 동작을 보다 상세히 설명하면, 컴퓨터 시스템을 구성하는 요소들로는 중앙처리장치(CPU), 램(RAM), 하드디스크(HDD), 및 각종 장치들이 있다. 본 발명에서 제안하는 시스템 고유 정보에 의한 사용자 고유 키 생성은 이러한 각 사용자의 시스템 구성 요소들의 고유 정보를 이용하여 사용자 고유 키를 생성하며, 이를 통해 사용자 인증 및 정보 사용 재생 여부를 제어한다.

<55> 보다 상세히 설명하면, 중앙처리장치의 경우 펜티엄 Ⅲ 이상의 칩은 고유 ID를 가지고 있다. 또한 하드디스크는 그 마스터 영역의 물리적인 섹터를 조사하면 제조사 정보(IDE)를 찾을 수 있다. 제조사 정보에는 제조사명, 시리얼 번호, 기종 등에 관한 정보들이 포함되어 있다. 시리얼 넘버 등의 경우에는 제조사A, 제조사B 등에서 사용하는 넘버가 동일하게 겹칠 수도 있다. 본 발명에서는 이와 같이 시스템의 특성들을 나타내는 정보들을 추출하며, 이렇게 추출된 시스템 고유 정보를 근거로 사용자 고유 키를 생성한다.

<56> 이러한 추출된 고유 정보를 외부적으로 확인할 수 없도록 차단하는 기능을 가지는 사용자 애플리케이션 툴(214)에서 공지의 블랙박스에 저장한 후, 이러한 고유 정보를 이용하여 사용자 고유 키를 생성한다. 사용자 고유 키의 생성을 위한 알고리즘은 다양한 방법에 의하여 구현될 수 있다. 생성된 사용자 고유 키는 보안유지를 위하여 레지스트리(registry)등에는 남아있지 않도록 하며 본 발명에서 제공하는 사용자 애플리케이션 툴(214)에서 정보를 요청할 때마다 사용자 고유키를 검색하여 암호화된 정보를 풀어준다. 물론 이 플러그 인에는 블랙박스가 내장되어 있도록 한다. 이상과 같은 일련의 과정에 의하여 특정 사용자가 인증한 정보는 규칙설정부(142)에서 정한 규칙에 의하여 제2, 제3의 사용자에게 재배포되어 인증된 허가없이 재사용될 수 없도록 제어된다.

<57> 이렇게 생성된 사용자 고유 키는 사용자 정보 DB부(146)로 전달되어 본 발명에 따른 시스템을 이용하는 사용자들에 대한 정보로서 관리된다. 따라서 사용자 관리 툴(132)은 사용자의 고유 키와 함께 사용자들에게 제공되는 디지털 정보에 대한 암호화를 위하여 생성되는 암호화 키 등에 대한 정보를 관리한다.

<58> 상기에서와 같이 디지털 정보의 사용에 대한 인증을 포함하여 서버제어부의 사용자 관리 툴(132)에서 사용자의 정보 요구에 대하여 사용자에 대한 인증이 이루어지면, 해당 사용자는 암호화가 이루어진 기업정보를 다운로드 등과 같은 절차를 거쳐서 받을 수 있다.

<59> 사용자 관리 툴(132)의 기본적 기능은 디지털 정보의 생성에서 배포, 사용, 폐기에 이르는 전 과정에 걸쳐서 정보의 불법배포나 불법사용을 막을 수 있도록 암호화 과정을 통해서 정보를 보호하고 이와 관련하여 정보의 저작권이나 기밀

등을 관리 및 보호해 주는 것이다. 암호화 키를 가진 적법한 사용자만이 암호화된 정보를 복호화하여 사용할 수 있으며, 불법 유통되어도 키가 없으면 사용할 수 없도록 함으로써 정보를 보호한다.

<60> 특히 본 발명에서는 암호화된 정보를 복호화하는 키를 사용자에게 전송함에 있어 사용자 애플리케이션 툴(214)을 통해 관리되도록 함으로써 그 보안성을 높여, 키가 유출되는 것을 방지하도록 한다. 암호화 키는 소정크기의 바이트 길이를 갖는(본 발명의 일 실시예에서는 128비트의 길이를 가지는) 암호화키가 이용될 수 있다. 이러한 암호화에는 상용화된 다양한 암호화 알고리즘을 사용할 수 있으며, 그 예로 투피쉬 암호화(Twofish encryption)알고리즘, 또는 블로우피쉬 암호화(Blowfish encryption)알고리즘 등을 예로 적용할 수 있다.

<61> 사용자는 정보를 사용할 때만 키를 이용하며, 정보는 항상 암호화되어 잠겨진 상태로 존재하고 사용시에만 사용자 애플리케이션 툴(214)을 통하여 사용자 고유 키와 기업문서 암호화 키의 인증을 통해 사용 가능한 형태로 제공된다. 이러한 정보 배포 및 인증 체계에서는 정보사용 관련 규칙을 규칙설정부(142)에서 설정하며, 이는 정보를 유통하고 사용할 때 각 개인의 사용 규칙과 권한을 나타내는 것이며, 디지털 정보의 저작권 보호와 직접적인 관련은 없다. 이러한 규칙 설정에 의하여 디지털 정보의 재분배에 따른 규칙의 추가나 수정 등 자유로운 규칙 관리를 통해 효율적인 정보를 제공하는 것이 가능하다. 사용자는 허가된 규칙에 의해서만 정보를 사용하는 것이 가능함은 물론이다.

<62> 이하 상기한 사용자 등록 및 기업정보의 업로드/다운로드에 대해 첨부 도면을 참조하여 상세히 설명하기로 한다.

<63> 도 3은 본 발명의 일 실시예에 따른 기업정보 서버(10)에서의 사용자 등록 과정의 동작 흐름도이다. 먼저 302단계에서 사용자가 기업정보 서버(10)에 접속하게 되면, 기업정보 서버(10)는 304단계에서 사용자의 사용자 애플리케이션 툴이 설치되었는지 여부를 확인하여 해당 접속한 사용자가 이미 등록된 사용자인지를 확인하고 등록된 사용자이면 이후 306단계로 진행하여 해당 기능을 수행하게 된다. 등록된 사용자가 아니면 이후 308단계로 진행하여 해당 사용자가 적합한 사용자인가를 인증하는 일련의 절차를 수행하게 된다. 해당 사용자가 적합한 사용자가 아닐 경우에는 이후 310단계로 진행하여 부적합한 사용자로서 이후 처리 동작을 수행하며, 적합한 사용자인 경우에는 312단계로 진행한다.

<64> 312단계에서는 사용자 애플리케이션 툴 프로그램을 사용자의 시스템으로 다운로드하여 자동으로 실행하도록 한다. 사용자 애플리케이션 툴이 사용자 시스템에 설치되면 사용자 애플리케이션 툴은 사용자의 시스템에서 고유 정보를 읽어서 이를 이용하여 사용자 고유 키를 생성한 후 이를 사용자 관리 툴로 전송하게 된다. 이에 따라 314단계에서 사용자로부터 사용자 고유 키 및 가 전송되면 기업정보 서버(10)는 316단계에서 해당 사용자 등록을 수행하고, 이후 318단계에서 등록된 사용자의 고유 키를 포함한 사용자 정보를 사용자 정보 DB(146)에 저장하게 된다. 이때 사용자 정보는 미리 설정된 적절한 암호화 알고리즘에 따라 암호화되어 저장되며, 이에 따라 해당 사용자 정보에 대한 정보가 유출되더라도 이를 해석될 수 없도록 한다.

<65> 상기 도 3에 도시된 바와 같은 과정은 사용자가 사용자의 고유 키를 등록하기 위해 사용자 애플리케이션 툴(214)을 설치하고 서버(10)에 사용자 고유 키를

전송하는 일련의 과정이다. 도 3에 도시된 바와 같이, 사용자가 본 발명의 일 실시예에 따른 시스템에 의하여 제공되는 서비스의 미등록자인 경우에는 먼저 사용자 등록과정을 거친다. 등록시에는 사용자 관리 툴(132)로부터 사용자 애플리케이션 툴을 받아서 사용자의 컴퓨터에 설치하게 되고, 등록된 사용자 고유 키, 즉 사용자의 인적사항 또는 사용하는 컴퓨터에 대한 자료가 LAN이나 인터넷을 이용한 WWW 등을 통하여 사용자 관리 툴(132)로 전송되어 사용자의 정보를 암호화 한 후, 별도의 데이터베이스, 즉 사용자정보 DB(146)에 저장된다.

<66> 도 4는 본 발명의 일 실시예에 따른 기업정보 서버(10)에서의 사용자로부터의 기업문서 업로드 과정의 동작 흐름도이다. 도 4를 참조하면, 먼저 402단계에서 사용자가 서버에 접속하면, 사용자 관리 툴에서는 404단계에서 우선적으로 사용자의 시스템에 사용자 애플리케이션 툴이 설치되어 있는지를 확인하여 사용자 등록 여부를 확인하고 설치되지 않은 경우는 406단계로 진행하여 상기 도 3에 개시된 바와 같은 사용자 등록과정을 거치도록 한다. 사용자 애플리케이션 툴이 설치된 경우는 이후 408단계로 진행하여 사용자 고유 키를 읽어서, 이를 사용자 정보 DB의 기 저장된 해당 사용자 정보와 비교하여 사용자가 시스템 사용에 적합한 가를 인증하게 된다. 사용자가 시스템 사용에 적합하지 않을 경우에는 이후 410단계로 진행하여 사용자 인증 불가 처리 동작을 수행하며, 사용자가 인증된 경우에는 이후 412단계로 진행하여 해당 사용자가 파일의 업로드가 가능하도록 허가한다.

<67> 이에 따라 업로드된 문서는 사용자의 정보와, 기업문서 정보, 기업문서로 각각 구분되어 각각 414, 424, 434단계에서 암호화된 후, 각각 416, 426, 436단계에서 사용자정보 DB, 기업문서정보 DB, 및 기업문서 DB에 저장된다. 이후 440단계에 해당 기업문서의 규칙을 설정하는 내용이 추가되며, 이후 442단계에서는 결합부에서 각각 합쳐지며, 이후 444단계에서 암호문서 DB에 암호화된 기업문서로서 저장된다.

<68> 상기 도 4에 도시된 바와 같은 과정을 살펴보면, 사용자가 사용자 관리 툴(132)을 통하여 LAN 상에서 또는 웹 서비스에 접속하여 사용자 인증 등의 과정을 거친 후에 올리고자 하는 기업문서를 서버(10)에 올리면, 디지털 기업문서 정보는 DB 게이트웨이(도 2의 인터페이스부 141)를 통해 입력되어 암호부(143)에 의해 암호화된 후 기업문서정보 DB(147)로 저장되고, 기업문서 파일은 암호부(143)를 통해 암호화키로 암호화된 후 기업문서 DB(148)에 저장된다. 사용자의 고유키 정보는 사용자 정보 DB(146)에서 읽혀져서 규칙설정부(142)에 의해 규칙 DB(149)의 설정사항에서 설정된 규칙을 가지고 결합부(144)로 전송된다. 결합부(144)에는 상기 각 데이터베이스에 저장된 사용자 고유 키와, 규칙, 기업문서 정보, 기업문서를 결합하고, 결합된 정보는 암호문서 DB(145)에 저장된다.

<69> 상기에서 업로드된 문서의 처리 동작을 보다 상세히 살펴보면, 상기 도 2에 도시된 바와 같은, 서버 제어부(150)의 업/다운 처리부(134)에 문서가 업로드되는 경우에, 업로드된 정보를 암호부(143)에 전달하게 된다. 암호부(143)는 전달받은 정보를 이용하여 실제 기업문서가 업로드 된 위치를 액세스하여 업로드된 문서를 액세스하고, 각 문서마다 별도의 키(예를 들어 128비트 암호화 키)를 생

성하고 이를 해당 문서 정보와 함께 내부 데이터베이스에 저장한다. 이후 암호부(143)는 상기 문서 키를 이용하여 해당 문서를 암호화한다. 이와 같이 문서를 미리 암호화하는 이유는 다음과 같다. 첫째 사용자가 해당 문서를 다운로드시 암호화에 따른 시스템 부하를 최소화하며, 둘째 문서 자체에 대한 암호화를 수행하지 않으므로 처리 속도 최대화하며, 셋째 고의 또는 실수로 인해 문서가 공개되는 경우 암호화되어 있어 문서의 보안이 유지되도록 한다. 이후 암호부(143)는 해당 암호화한 문서를 지정된 데이터베이스의 폴더에 저장한다. 이후 암호부(143)는 업로드 처리, 즉 사용자로부터 전송된 파일을 암호화한 처리가 완료되었음을 업/다운 처리부(134)로 통지한다.

<70> 도 5는 본 발명의 일 실시예에 따른 기업정보서버에서의 사용자로 기업문서 다운로드 과정의 동작 흐름도이다. 도 5를 참조하면, 먼저 502단계에서 사용자가 서버에 접속하면, 사용자 관리 툴에서는 504단계에서 우선적으로 사용자의 시스템에 사용자 애플리케이션 툴이 설치되어 있는지를 확인하여 사용자 등록 여부를 확인하고 설치되지 않은 경우는 506단계로 진행하여 상기 도 3에 개시된 바와 같은 사용자 등록과정을 거치도록 한다. 사용자 애플리케이션 툴이 설치된 경우는 이후 508단계로 진행하여 사용자 고유 키를 읽어서, 이를 사용자 정보 DB의 기 저장된 해당 사용자 정보와 비교하여 사용자가 시스템 사용에 적합한 가를 인증하게 된다.

사용자가 시스템 사용에 적합하지 않을 경우에는 이후 510단계로 진행하여 사용자 인증 불가 처리 동작을 수행하며, 사용자가 인증된 경우에는 이후 512단계로 진행하여 해당 사용자의 기업문서 다운로드 요청을 받아들인다. 이후 514단계에서 해당 기업문서를 사용자 애플리케이션 툴로 전송한다.

<71> 사용자 애플리케이션 툴에서는 이후 520단계에서 상기와 같이 서버로부터 다운로드된 문서에 포함되어 있는 사용자 고유 키와 자신이 생성한 사용자의 고유키가 일치하는가를 확인한다. 일치하지 않을 경우에는 이후 522단계로 진행하여 고유 키 불일치 처리 동작을 수행하며, 일치하는 경우에는 이후 524단계로 진행한다. 524단계에서는 다운로드받은 기업문서에 포함된 복호화 키를 복호화할 수 있는 키로 변환하여 복호화가 가능한지를 확인한다. 복호화가 불가능할 경우에는 이후 526단계로 진행하여 복호화 불가능 처리 동작을 수행하며, 복호화가 가능할 경우에는 이후 530단계로 진행 해당 기업문서에 포함된 암호화 키를 사용하여 기업문서의 복호화를 수행한다. 이후 532단계에서는 상기 복호화된 기업문서를 출력하여 열람, 수정, 또는 저장이 가능하도록 한다.

<72> 상기에서 문서 다운로드의 동작을 보다 상세히 설명하기로 하면, 사용자가 특정한 파일을 선택하면 선택된 정보는 업/다운 처리부(134)에 전달된다. 업/다운 처리부(134)는 상기 선택된 파일에 대한 정보를 결합부(144)로 전달한다. 결합부(622)는 상기 전달받은 정보를 이용하여 다운로드할 암호화된 파일을 물리적으로 액세스하고, 사용자 고유 ID DB), 문서키, 규칙 등에 대한 정보를 얻어와 사용자의 권한에 맞는 암호화된 다운로드 문서 파일을 사용자 애플리케이션 툴(214)

에 생성한다. 이후 결합부(144)는 상기 암호화된 다운로드 문서 파일을 다운로드 위치에 저장한다. 결합부(144)는 저장이 완료되면 업/다운 처리부(134)에 동작 수행이 완료되었음을 통지한다. 이에 따라 업/다운 처리부(134)는 일반적인 다운로드 처리 동작을 수행하여 상기 암호화된 다운로드 파일의 전달받아 실제 사용자에게 파일을 다운로드 한다.

<73> 상기 도 5에 도시된 바와 같은 과정을 다시 살펴보면, 사용자로부터 특정 디지털 정보에 대한 요구가 있는 경우에 사용자 관리 툴(132)은 사용자 인증과정을 거친 후에 암호문서 DB(145)에 저장된 암호화된 기업문서를 해당 사용자의 사용자 애플리케이션 툴(214)로 전송한다. 암호화된 기업문서는 사용자의 요청에 따라 LAN이나 인터넷 등을 통하여 전송된다.

<74> 사용자는 이 암호화된 기업문서파일을 재생하기 위하여 복호화 과정을 거쳐야 한다. 이때, 이 정보를 재생하기 위하여 정보 복호화 키가 필요한데, 복호화에 필요한 키는 상기 언급한 해당 정보 사용자의 고유 키로 암호화되어 제공된다. 즉 사용자의 고유 키로 암호화된 기업문서 파일의 복호화 키가 제공되는 것이다.

<75> 따라서, 해당 디지털 정보가 사용자에게 전송되어 해당 정보를 재생하기 위해서는 암호화된 정보와 함께 전송된 복호화 키를 사용하여 정보를 복호화 할 수 있는가의 여부가 중요하다. 즉 정보를 재생하기 위해서는 정보를 복호화 하는 키가 필요한데, 이 복호화 키 역시 암호화되어 사용자에게 전송되므로 이 키를 복호화 하는 과정이 먼저 진행되어야 하는 것이다.

<76> 암호화된 정보를 복호화 할 수 있는 키는 사용자의 시스템 고유 정보로부터 사용자 애플리케이션 툴(214)을 통해 추출된다고 할 수 있다. 즉 처음에 정보를 사용하는 사용자가 시스템 정보로부터 추출한 고유 정보로 사용자 고유키를 만들어서 정보 복호화 키를 암호화하기 때문에 이를 다시 복호화하기 위해서는 다른 사용자의 시스템 정보로부터 생성된 사용자 고유 키와 정보 복호화 키를 암호화한 키가 일치하는지의 여부를 체크하여 일치하여야 하는 것이다. 만약, 상기 체크 시에 암호화된 기업문서 파일 복호화 키를 암호화하는 키와 사용자의 고유 키가 동일하지 않는 경우에는 사용자는 정당한 사용권자가 아님을 알리는 메시지의 표시와 함께 작업이 종료된다.

<77> 그런데, 암호화된 기업문서파일의 복호화 키를 암호화하는 키와 사용자의 시스템에서 추출, 생성된 사용자 고유 키가 일치하는 경우에는 사용자의 시스템 고유 키로 암호화 된 기업문서의 복호화 키를 사용하여 정보 복호화 키를 추출해 낼 수 있게 된다. 이렇게 추출된 정보 복호화 키를 이용하여 기업문서 파일을 복호화하고 사용자 애플리케이션 툴(214)을 사용하여 기업 정보를 재생한다.

<78> 한편, 디지털 정보가 배포되는 경로는 유, 무선 통신을 이용하여 온라인 상의 경로를 이용할 수도 있지만, 필요에 따라 오프라인 상의 직접적 전달 경로를 이용할 수도 있다. 상기 본 발명의 일 실시 예에 대한 설명에서는 디지털 정보의 제공, 구매 등이 온라인 상에서 이루어지고 일련의 프로그램이나 정보의 다운로드 역시 온라인 상으로 이루어지는 것을 중심으로 설명하였으나, 상황에 따라 상기 디지털 정보들은 플로피 디스크, CD(Compact Disc), DVD ROM, "Zip"

디스크, 레이저 디스크, 혹은 비디오테이프나 카세트테이프 등 저장 매체를 통해 저장되어 오프라인 상으로 유통될 수도 있다.

<79> 이와 같이, 디지털 정보가 오프라인 상으로 유통되는 경우에도 최초로 사용자가 자신의 컴퓨터 등 단말기에서 정보를 오픈하거나 재생시, 사용자 애플리케이션 툴의 실행을 통해 사용자 고유 키를 생성하고 생성된 사용자 고유 키에 의하여 이후 정보 재생 여부를 판단, 제어할 수 있도록 한다.

<80> 이러한 과정을 통해 저장매체를 사용하여 파일을 다운로드 하여 기업문서를 누출시키고자 하는 경우에도 해당 사용자 단말기에 설치된 사용자 애플리케이션 툴에 의해서만 기업문서의 열람, 수정, 혹은 저장 및 출력이 가능하기 때문에 저장 매체를 통한 기업문서 정보의 누출이 불가능하게 된다.

<81> 도 6은 본 발명의 다른 실시 예에 따른 디지털 정보 보안 시스템의 개략적인 전체 블록 구성도이다. 도 6에 도시된 바와 같은 본 발명의 다른 실시 예에 따른 디지털 정보 보안 시스템은 상기 도 2 등에 개시된 바와 같은 본 발명의 일 실시 예와는 달리 사용자가 접속하는 웹 서버와, 본 발명의 특징에 따른 동작을 수행하기 위한 문서 보안을 위한 시스템은 서로 분리되어 있으면 양자 간에는 소켓 통신을 통해 서로 연결되도록 한다. 또한 이때의 웹서는 일반적인 지식 관리 또는 문서 관리 시스템의 일부분일 수 있다.

<82> 도 6을 참조하면, 본 발명에 따른 디지털 정보 보안 시스템은 크게 3개의 서비스 모듈 즉, 문서키 관리 서비스모듈(Document Key Management Service :

DKMS)(610)과, 문서배포 서비스모듈(Document Distribution Service : DDS)(620) 및 문서관리 서비스 게이트웨이(Document Management Service Gateway : DMSG)(630)와, 문서관리 시스템 또는 지식관리시스템에 포함될 수 있는 업/다운 처리를 위한 웹서버(640)로 구성된다.

<83> 문서키 관리 서비스모듈(610)은 사용자의 정보 및 사용자 고유 ID(User Unique ID : UUID)를 관리하는 서비스 모듈이다. 사용자 고유 ID는 상기 도 1 및 도 5에 개시한 바와 같은 사용자 개인용 컴퓨터와 같은 사용자 시스템 정보를 바탕으로 만들어진다.

<84> 문서배포 서비스모듈(620)은 사용자가 문서를 다운로드 받을 때 동작하며, 프린트 권한, 저장 권한, 복사 권한 등의 사용자 권한 등과 같은 각종 사용자 환경에서의 해당 문서의 출력 규칙에 대한 정보를 포함한 암호화된 문서를 만들어 낸다.

<85> 문서관리 서비스 게이트웨이(630)는 사용자가 문서를 지식관리 시스템이나 문서관리 시스템으로 업로드(upload)할 때 동작한다. 문서관리 서비스 게이트웨이는 각 문서별 문서 키를 생성하고 이를 이용하여 문서를 암호화하는 동작을 수행한다.

<86> 웹서버(640)는 지식관리 시스템(KMS) 또는 문서관리 시스템에 포함될 수 있는 시스템으로서 업로드 프로세스 처리 시에는 사용자가 업로드 한 문서의 정보를 문서관리 서비스 게이트웨이(630)로 전송한다. 또한 다운로드 프로세스 처리 시에는 사용자가 특정 파일을 요청할 시 해당 요청에 대한 정보를 문서배포

서비스모듈(620)로 전송한다. 이하의 설명에서 일반적인 웹서버의 기능으로서 파일 업/다운로드에 관련된 기능에 관한 처리는 업로드/다운로드 프로세스라 칭하며, 본 발명의 특징에 따른 파일 업/다운에 관련되는 기능을 수행하는 기능부는 업/다운로드 처리부라 칭한다.

<87> 도 7은 도 6 중 문서키 관리 서비스 모듈(610)의 동작을 설명하기 위한 도면이다. 문서키 관리 서비스모듈(610)은 사용자의 정보와 사용자 고유 ID를 관리하는 모듈이다. 사용자 고유 ID는 사용자의 초기 등록시 사용자의 시스템에 설치되는 사용자 애플리케이션 툴로부터 해당 사용자의 시스템 정보를 기반으로 생성되어지며, 이후 웹서버(640)에서는 이를 이용하여 문서를 암호화한 후 사용자에게 내려 보내주게 된다. 사용자 고유 ID는 시스템 고유 정보이므로 타 사용자와 중복될 수 없다. 해당 사용자의 시스템에 설치되는 사용자 애플리케이션 툴은 초기 설치 시와 시스템 업그레이드 등의 동작 시에는 해당 사용자 정보와 사용자 고유 ID를 문서키 관리 서비스모듈(610)로 다시 재 전송한다.

<88> 도 7을 참조하면, 사용자 측에서 전송된 정보는 이후 문서키 관리 서비스모듈(610)에서 128비트 NIST 공인 암호화 모듈인 프로파일 암호화기(612)를 통해 암호화되어 데이터베이스(UUID DB(614))에 안전하게 저장된다. 이에 따라 해당 사용자 정보 및 사용자 고유 ID에 대한 정보가 유출되더라도 이를 해석될 수 없게 된다.

<89> 도 8은 도 6중 문서관리 서비스 게이트웨이(630)의 동작을 설명하기 위한 도면이다. 도 8을 참조하면, 문서관리 서비스 게이트웨이(630)는 사용자로부터 보안을 요하는 파일이 업로드 되는 시점에서부터 실시간 문서 암호화 및 관리를 위해 사용되는 서비스 모듈로써 TCP/IP를 통해 데이터를 전송하도록 하여 서버제어부(130) 및 데이터 저장부(140)등의 시스템과의 연동이 자유스러우며 간단한 시스템 파일 또는 서버측에서 DLL형태의 파일로 제공되어지는 업로드 프로세스와 함께 동작하도록 설계되어 있다.

<90> 문서관리 서비스 게이트웨이(630)의 동작을 살펴보면, 먼저 801단계는 지식관리시스템(KMS) 또는 문서 관리 시스템에 추가되는 모듈로써 웹서버(640)의 업로드 처리부(642)에 의해 파일이 업로드 되는 경우에, 이러한 업로드에 대한 정보를 TCP/IP를 통해 전달받게 된다. 이후 802단계에서는 전달받은 정보를 이용하여 실제 파일이 업로드 된 위치를 액세스하여 업로드된 파일을 액세스하고, 이를 문서키 발생기(632)로 전달한다. 문서키 발생기(632)는 각 문서마다 별도의 키를 생성하는 모듈로써 128비트 암호화 키를 생성하고 이를 해당 문서 정보와 함께 데이터베이스(문서키 DB(636))에 저장한다.

<91> 이후 803단계에서는 문서 암호화기(634)는 상기 문서키 발생기(632)에서 발급한 문서키를 이용하여 해당 문서를 암호화한다. 이와 같이 문서를 미리 암호하는 이유는 다음과 같다. 첫째 사용자가 해당 문서를 다운로드시 암호화에 따른 시스템 부하를 최소화하며, 둘째 문서 자체에 대한 암호화를 수행하지 않으므로 처리 속도 최대화하며, 셋째 고의 또는 실수로 인해 파일이 공개되는 경우 암호

화되어 있어 문서의 보안이 유지되도록 한다. 이후 문서 암호화기(634)는 해당 암호화한 문서를 지정된 암호문서 DB(145)의 폴더에 저장한다.

<92> 이후 805단계에서 문서 암호화기(634)는 업로드 처리, 즉 사용자로부터 전송된 파일을 암호화한 처리가 완료되었음을 해당 지식관리시스템(KMS) 또는 문서 관리 시스템에 통지한다.

<93> 도 9는 도 6중 문서배포 서비스 모듈(620)의 동작을 설명하기 위한 도면이다. 리스트뷰 프로세스(List View Process)(646)는 사용자에게 KMS 또는 문서 관리 시스템의 다운로드받을 항목을 보여주는 프로세스이다. 901단계에서 사용자가 이를 통해 특정한 파일을 선택하면 선택된 정보는 다운로드 처리부(648)로 전달된다.

<94> 다운로드 처리부(648)는 선택된 파일에 대한 정보를 수집한 후 902단계에서 TCP/IP 통신을 이용하여 해당 정보를 문서배포 서비스 모듈(620)로 전송한다. 문서배포 서비스 모듈(620)에서 결합기(622)는 시스템 다운로드 처리부(648)에서 전달 받은 정보를 이용하여 903단계에서 암호화된 파일을 물리적으로 액세스하고, 사용자 고유 ID DB(614), 문서키 DB(636), 규칙 DB(624)의 정보를 얻어와 사용자의 권한에 맞는 암호화된 다운로드 문서 파일을 사용자 애플리케이션 툴(214)에 생성한다.

<95> 이후 결합기(622)는 904단계 상기 암호화된 다운로드 문서 파일을 다운로드 위치에 저장한다. 결합기(622)는 파일이 저장이 완료되면 이후 905단계에서 다운

로드 처리부(648)에 동작 수행이 완료되었음을 통지한다. 이에 따라 다운로드 처리부(648)는 906단계에서 KMS 또는 문서 관리 시스템의 파일 다운로드 프로세스(644)로 작업을 이관한다. 이후 907단계에서 다운로드 프로세스(644)는 상기 암호화된 다운로드 파일의 전달받아 실제 사용자에게 파일을 다운로드 한다.

<96> 한편, 최근 들어 많은 기업이나 관공서, 학교 등은 기업환경을 기존의 클라이언트/서버 구조에서 웹 환경으로 대치하고 있다. 웹 인터페이스를 지원하는 응용 프로그램의 경우에는 별도의 프로그램을 설치하거나 업데이트 하지 않아도 되므로 유지보수가 간편하며, 언제 어디에서나 시스템을 관리할 수 있다는 장점을 가지고 있다.

<97> 따라서 본 발명의 특징에 따른 디지털 정보 보안 시스템은 이러한 웹의 장점을 도모하고자 도 2 및 도 6에 도시된 바와 같은 사용자 관리 툴(132)을 웹을 통해 액세스 할 수 있도록 구성한다. 이는 시스템간의 이 기종 포팅이 가능하도록 설계되어 관리 툴의 설치를 용이하게 한다.

<98> 도 10은 본 발명의 일 실시예에 따른 디지털 정보 보안 시스템에서 사용자 관리 툴의 운영자 인터페이스 화면의 예시도이다. 도 10을 참조하면, 운영자 인터페이스 화면에는 각 사용자의 ID 및 해당 사용자의 부서와 직급 등을 입/출력하기 위한 근무처 관리란과, 각 사용자별 권한 및 규칙에 대한 설정을 입/출력하기 위한 규칙관리란과, 전체 부서 조직에 대해 트리구조로 나타내어지는 전체 조직관리란과, 특정 그룹에 속한 하부 부서 조직에 대해 텍스트윈도우 형태로 나타내어지는 하부조직 관리란 등으로 구성될 수 있다. 이때 해당 부서의 모든 사람

에 모든 권한을 설정해 주기 위한 전체 권한 단추나 특정 부서의 추가를 위한 부서 추가 단추 등이 더 구성될 수 있다.

<99> 도 11a는 도 10의 관리 툴 인터페이스 화면 중 해당 부서의 모든 사람에게 모든 권한을 부여하기 위한 화면의 예시도이며, 도 11b는 도 10의 관리 툴 인터페이스 화면 중 해당 부서의 모든 사람에게 모든 권한이 부여된 상태를 나타내는 화면의 예시도이다. 도 11a, 11b를 참조하면, 관리자가 도 10에 도시된 바와 같은 화면상의 전체 권한 단추를 클릭하였을 경우에, 도 11a에 도시된 바와 같은 확인 입력 윈도우가 출력되며, 관리자가 이러한 윈도우에서 확인 단추를 클릭하였을 경우에 도 11b에 도시된 바와 같은 모든 해당 부서의 무든 사람에게 모든 권한이 부여된 상태의 화면이 출력될 수 있다. 이러한 모든 권한의 부여 표지는 규칙 관리란에서 모든 권한이 'V'표로 표시된 상태로 출력된다.

<100> 도 12a는 도 10의 관리 툴 인터페이스 화면 중 새로운 부서를 추가하기 위한 화면의 예시도이며, 도 12b는 도 10의 관리 툴 인터페이스 화면 중 새로운 부서가 추가된 상태를 나타낸 화면의 예시도이다. 도 12a, 12b를 참조하면, 관리자가 도 10에 도시된 바와 같은 화면상에서 부서 추가 단추를 클릭하였을 경우에 해당 부서명을 입력하기 위한 입력 윈도우가 출력된다. 도 12a에는 추가 부서명으로 "SI 사업부" 를 입력한 상태가 도시되며, 도 12b에는 "SI 사업부" 가 트리 구조의 전체 조직 관리란에 하위 폴더로, 또한 하부 조직 관리란의 특정 라인에 추가된 상태가 도시된다.

<101> 도 13a는 도 10의 관리 툴 인터페이스 화면 중 특정 사용자의 사용자 정보의

변경을 위한 화면의 일 예시도이며, 도 13b는 도 10의 관리 툴 인터페이스 화면 중 특정 사용자의 사용자 정보의 변경을 위한 화면의 다른 예시도이다. 도 13a, 13b를 참조하면, 도 10에 도시된 바와 같은 각 사용자별 근무처 관리란은 해당 사용자별로 부서 및 직급을 입력하는 란으로 구성될 수 있다. 이때 관리자는 도 13에 도시된 바와 같은 각 사용자의 부서란을 클릭하여 부서명을 변경할 수 있고 도 13b에 도시된 바와 같은 직급란을 클릭하여 해당 사용자의 직급을 변경할 수 있다.

<102> 이러한 관리자에 의한 부서 변경 및 직급 변경을 통해 해당 사용자는 자신이 속한 부서의 문서만 보거나 직급별 문서 접근 권한이 설정될 수 있다.

<103> 한편, 상기한 바와 같은 본 발명의 특징에 따른 디지털 정보 보안 시스템에서 상기 도 10에 도시된 바와 같은 규칙 관리란 등에서 설정되는 바와 같은 규칙들에는 하기와 규칙을 포함할 수 있다.

<104> 1) 저장 권한 : 다운로드 받은 파일을 원래 파일 포맷으로 자신 컴퓨터에 저장할 수 있는 권한으로서, 다운로드 받은 문서를 저장하는 경우에는 사용자의 컴퓨터에 해당 포맷의 일반적인 문서로 저장할 것인지, 아니면 암호화된 상태로 저장하게 할 것인지 지정할 수 있다. 도 14a는 문서 저장 권한이 없는 사용자가 해당 문서의 저장을 시도한 경우의 출력 화면의 예를 나타낸다.

<105> 2) 프린트 권한 : 다운로드 받은 파일의 출력 권한 부여 및 횟수에 관한 권한으로서, 실제 전자적인 데이터의 유통 이외에 기업 내부에서 관리해야 할 부분

으로 중요한 부분이 프린터를 이용한 출력물에 대한 제어이다. 출력물은 손쉽게 복사될 수 있으며 타인에게 배포될 수 있다. 이러한 점을 막기 위하여 본 발명에서는 출력 가능 여부 및 출력 횟수에 대한 정보를 지정, 관리할 수 있도록 하였다. 도 14b는 프린트 권한이 없는 사용자가 프린트를 시도한 경우의 출력 화면의 예를 나타낸다.

<106> 3) 사용기간 권한 : 다운로드 받은 파일의 사용할 수 있는 기간에 관한 권한으로서, 다운로드 받은 문서는 실질적으로 사용기간에 대한 제한을 부여할 수 있으며 사용 기간이 지난 문서는 자동으로 폐기 될 수 있다. 폐기의 시점에 관해서는 본 발명에 의한 관리 툴 인터페이스 화면을 각 기업의 업무에 맞게 커스터마이징할 때 구현된다.

<107> 4) 양도 권한 : 다운로드 받은 파일을 다른 사람에게 양도할 수 있는 권한으로서, 다운로드 받은 문서는 타인에게 양도될 수 있으며(권한이 있는 경우) 이 때 여러가지 방법이 지원될 수 있다. 상대방이 직접 문서 권한을 가진 사용자에게 자신의 정보를 알려 주어 별도의 관리 툴 인터페이스가 개입하지 않고 동작할 수도 있으며, 양도시는 관리 툴 인터페이스에 항시 접속하도록 구성할 수 있다. 이 부분도 기업의 정책에 따라 커스터마이징 된다.

<108> 이와 같은 권한 부여는 상기 설명한 바와 같이 관리자에 의해 이루어지는데, 실제로 기업 내부의 사용자들에 대한 권한 부여는 관리자에게 많은 업무를 가중시킬 수 있으며, 빈번한 조직간의 이동으로 인해 관리가 힘든 부분이 발생할 수 있다. 이러한 부분을 해결하기 위하여 사용자별 규칙제한을 문서

의 등급에 따른 규칙 제한으로 변경할 수 있다. 즉, 문서의 보안 등급에 따라서 출력 및 저장 등을 지원하게 함으로써 관리자들의 개입을 최소화 할 수 있다.

<109> 이와 같이 본 발명의 특징에 따른 디지털 정보 보안 시스템은 다운로드 받는 문서를 사용자 권한에 따라 복사, 출력 및 다른 사람에게 배포 등을 제어할 수 있다. 이러한 사용자 권한은 기존의 지식관리 시스템이나 EDMS 시스템의 사용자 접근 제어 규칙을 그대로 연계해 처리할 수 있으며, 별도의 규칙 데이터베이스를 구성하여 운영할 수 있다.

<110> 상기한 바와 같이 본 발명에 따른 디지털 정보 보안 시스템은 기존의 지식관리 시스템이나 문서관리 시스템에 저장되는 원천 문서에 대해 NIST에서 공인한 암호화 알고리즘을 이용하여 보안상태를 유지하고, 사용자가 다운로드 받는 시점에서 해당 사용자만 열어 볼 수 있는 권한을 부여하여 다운로드 하므로 데이터의 외부 유출을 원천적으로 방지할 수 있다. 도 15는 본 발명의 일 실시예에 따른 문서 뷰어를 이용한 문서를 일반 문서 제작 프로그램을 통해 오픈한 경우의 예시 화면이다.

<111> 또한, 다운로드 받은 파일은 등록되지 않은 사용자가 열어볼 경우 의미없는 문서의 형태로 나타나며, 이를 내부의 다른 사용자에게 전달하는 경우에도 보안 관계(Trust Relationship)가 형성되지 않으면 열어볼 수 없는 구조로 설계된다. 도 16은 본 발명의 일 실시예에 따라 다운로드 받은 파일을 복사 및 다른 시스템에서 오픈한 경우의 출력 화면의 예시도이다.

<112> 한편, 일반적인 DRM 시스템이나 문서 보안 관리 시스템의 경우에는 별도의 응용 프로그램을 이용하여 암호화된 문서를 볼 수 있도록 하고 있다. 이러한 경우 문서 파일 포맷이 추가되거나 버전업되는 경우에는 별도의 문서 뷰어(viewer)를 제작, 배포하여야 하며 클라이언트는 이를 설치해야 하는 문제점을 가지고 있다. 또한 최근에는 파일 포맷이 복잡해져서 일반적인 DRM 업체에서 항시 버전업되는 파일에 대한 뷰어의 업데이트가 원활하게 이루어지지 않고 있는 상황이다.

<113> 본 발명에 따른 문서 뷰어 모듈의 경우에는 사용자 애플리케이션 툴에 설치되어, 도 17a와 같이 마이크로소프트 오피스 프로그램과 같은 문서 편집용 소프트웨어를 호출, 사용하는 구조로 설계되어 있어, 사용자들은 별도의 뷰어 소프트웨어나 플러그인이 없어도 상기 문서 편집용 소프트웨어를 그대로 사용할 수 있다. 즉, 본 발명에 따른 문서 뷰어 모듈은 각각의 문서 편집용 소프트웨어를 호출하여 특정한 윈도우에 출력시켜서 해당 문서 편집용 소프트웨어를 통해 사용자가 문서를 보거나 편집할 수 있도록 하며, 문서를 작성할 수 있도록 한다. 이때 사용자는 해당 문서 편집용 소프트웨어를 본 발명의 문서 뷰어 모듈을 통하지 않고 실행하는 경우와 거의 동일하게 실행시킬수 있다. 단 본 발명의 문서 뷰어 모듈은 해당 문서 편집용 소프트웨어의 실행시에 다운로드 받은 파일의 저장이나 프린트 등의 몇몇 미리 문서 보안을 위해 미리 제한을 둔 제한 동작 지시시에 이를 확인하여 상기 해당 사용 규칙설정에 따른 권한과 해당 사용자정보에 따라 파일 저장이나 프린트 등의 동작 수행 여부를 결정하게 된다. 도 17a, ~ 17e는 각각 본 발명의 일 실시예에 따른 문서 뷰어모듈을 이용하여 "POWERPOINT' 파일,

" MS-WORD' 파일, 'EXCEL' 파일, "훈민정음" 파일 및 "AutoCAD' 파일을 오픈한 경우의 출력 화면의 예시도이다.

<114> 일부 디지털 정보 보안 시스템 시스템들이 지원하는 플러그-인 방식의 응용 프로그램을 사용하는 경우에는 응용 프로그램이 버전업됨에 따라 항상 디지털 정보 보안 시스템 제공 업체에서 플러그-인을 제작 배포해야 하는 문제점을 가지고 있으나, 본 발명의 특징에 따른 문서 뷰어의 경우에는 사용자들이 단지 자신의 응용 프로그램만 업그레이드하면 되는 방식이므로 사용자 유지보수성 부분에서도 다른 문서관리 시스템의 경우와 차별화 된다 할 수 있다.

<115> 상기와 같은 구성에 의해 본 발명의 특징에 따른 디지털 정보 보안 방법 및 그 시스템이 이루어질 수 있으며, 상기한 본 발명의 설명에서는 구체적인 실시예에 관해 설명하였으나 여러 가지 변형이 본 발명의 범위를 벗어나지 않고 실시될 수 있다. 따라서 본 발명의 범위는 설명된 실시예에 의하여 정할 것이 아니고 청구범위와 청구범위의 균등한 것에 의하여 정하여져야 할 것이다.

【발명의 효과】

<116> 상기한 바와 같이 본 발명은 기업 내의 문서와 데이터 등과 같은 정보들의 불법적인 배포를 원천적으로 방지할 수 있을 뿐만 아니라 기업에서 사용자의 제한 및 자료공유를 위해 구축하는 통상의 KMS 구축과 연동시켜 시스템을 구동함으로써 기업 내의 정보나 자료가 자유롭게 왕래하면서도 외부로 누출되는 것을 방

지할 수 있다. 또한 KMS가 구축되지 않은 기업의 경우에도 LAN이나 WAN등에서 이를 활용하여 기업내의 문서유출을 방지할 수가 있다. 사용자가 기업문서를 저장매체를 통하여 외부로 누출시키고자 하는 경우에도 사용자 고유 키가 컴퓨터마다 다르기 때문에 사용할 수가 없다.

<117> 또한 외부에서 불법적인 해커 등에 의하여 기업문서의 DB가 해킹 당하는 경우에도 암호화된 기업문서이기 때문에 이를 사용할 수가 없다. 따라서 외부의 불법적인 침입에도 안전한 기업문서의 보안 시스템을 운영할 수가 있다.

【특허청구범위】

【청구항 1】

디지털 정보 보안 시스템에 있어서,

사용자 단말에 설치되며, 상기 사용자 단말의 시스템 고유 정보를 이용하여 해당 사용자의 고유 키를 생성하는 사용자 애플리케이션 툴과,

사용자 정보 및 디지털 정보를 저장하는 데이터 저장부와,

서버에 설치되며, 상기 사용자 애플리케이션 툴에서 생성한 상기 사용자 고유 키를 제공받아 이를 상기 데이터 저장부에 해당 사용자 정보의 일부로써 저장토록 하며, 사용자 인증시에 상기 저장된 사용자 고유 키와 현재 인증하는 사용자의 상기 사용자 애플리케이션 툴에서 제공되는 사용자 고유 키의 일치 여부를 비교하는 사용자 관리 툴을 포함하여 구성함을 특징으로 하는 보안 시스템.

【청구항 2】

제1항에 있어서, 상기 사용자 관리 툴은 상기 디지털 정보의 사용자에게로 다운로드시에 해당 사용자의 상기 사용자 정보에 포함된 사용자 고유 키를 포함하여 전송하며,

상기 사용자 애플리케이션 툴은 상기 디지털 정보를 다운로드받을 시에 상기 전송받은 사용자 고유 키와 자신이 생성한 사용자 고유 키를 비교하여 해당

다운로드받는 디지털 정보의 출력 여부를 결정함을 특징으로 하는 보안 시스템.

【청구항 3】

제1항 또는 제2항에 있어서, 상기 보안 시스템은

상기 각 저장된 디지털 정보에 대해 미리 설정된 사용자 규칙에 따라 규칙을 설정하는 규칙설정부를 추가로 더 가지며,

상기 사용자 관리 툴은 상기 디지털 정보의 사용자에게로 다운로드시에 해당 사용자에 대한 상기 규칙설정부에서 설정한 규칙 정보를 포함하여 전송하며,

상기 사용자 애플리케이션 툴은 상기 디지털 정보를 다운로드받을 시에 상기 전송받은 규칙 정보에 따라 해당 다운로드받는 디지털 정보의 출력 여부를 결정함을 특징으로 하는 보안 시스템.

【청구항 4】

제1항 또는 제2항에 있어서, 상기 시스템 고유 정보는 상기 사용자 단말의 중앙처리장치의 고유 정보와, 하드디스크의 고유 정보 및 상기 단말의 시리얼 정보 중 적어도 하나를 포함함을 특징으로 하는 보안 시스템.

【청구항 5】

디지털 정보 보안 방법에 있어서,

서버에서 사용자의 접속시에 해당 사용자 단말의 시스템 고유 정보를 이용하여 생성된 사용자 고유 키를 읽어들이는 과정과,

상기 읽어들인 사용자 고유 키와 미리 저장된 현재 접속한 사용자에 대한 사용자 정보에 포함된 사용자 고유 키를 비교하여 상기 접속한 사용자의 적합 여부를 인증하는 과정과,

상기 인증한 사용자의 파일 업로드시에 해당 파일을 미리 설정된 암호화 키를 이용한 암호화 방식으로 암호화하여 상기 디지털 정보로써 저장하는 과정과

,

상기 인증한 사용자의 상기 디지털 정보의 다운로드 요청시에 해당 디지털 정보의 복호화 키를 상기 사용자 정보에 포함된 사용자 고유 키를 이용하여 암호화하여 해당 디지털정보와 더불어 다운로드하는 과정을 포함하여 구성함을 특징으로 하는 보안 방법.

【청구항 6】

제5항에 있어서,

상기 사용자 단말에서 상기 다운로드받은 디지털 정보의 암호화된 복호화 키를 상기 시스템 고유 정보를 이용하여 생성한 사용자 고유 키를 이용하여 복호화하여 상기 디지털 정보를 복호화하는 과정을 더 가짐을 특징으로 하는 보안 방법.

【청구항 7】

제5항에 있어서, 상기 서버에서 사용자의 접속시에 상기 접속한 사용자의 미등록시에 상기 사용자 단말의 시스템 고유 정보를 이용하여 해당 사용자의 고유 키를 생성 및 전송하기 위한 프로그램을 상기 접속한 사용자에게 전송하여 설치토록 하는 과정과,

상기 설치된 프로그램에 의해 상기 생성 및 전송된 사용자의 고유 키를 이용하여 해당 사용자를 등록하는 과정을 추가로 더 가짐을 특징으로 하는 보안 방법.

【청구항 8】

디지털 정보 보안 방법에 있어서,

사용자 단말에서 암호화된 디지털 정보의 재생시 해당 사용자 단말의 시스템 고유 정보를 이용하여 사용자 고유 키를 생성하는 과정과,

상기 사용자 단말에서 상기 디지털 정보에 포함된 암호화된 복호화 키를 상기 생성한 사용자 고유 키를 이용하여 복호화하는 과정과,

상기 복호화된 복호화 키를 이용하여 상기 디지털 정보를 복호화하는 과정을 가지며, 상기 암호화된 복호화 키의 암호화에 사용된 키와 상기 생성한 사용자 고유 키가 일치하지 않을 경우에 상기 암호화된 복호화 키의 복호화가 불가능함을 특징으로 하는 보안 방법.

【청구항 9】

디지털 정보 보안 시스템에 있어서,

사용자의 시스템에 설치되는 사용자 애플리케이션 툴로부터 해당 사용자의 시스템 정보를 기반으로 생성되어지는 사용자 고유 아이디를 포함하는 사용자 정보를 미리 설정된 방식으로 암호화하여 저장하며 관리하는 문서키관리 서비스 모듈과,

사용자로부터 파일이 업로드 되는 경우에 해당 파일에 대한 문서키를 생성하여 저장하며 상기 생성한 문서키를 이용하여 해당 파일을 암호화하는 문서관리 서비스 게이트웨이와,

사용자로 파일을 다운로드할 경우에 미리 설정된 사용자 환경에서의 해당 파일의 출력 규칙에 대한 정보를 포함한 암호화된 다운로드 파일을 생성하는 문서배포 서비스 모듈과,

인터넷을 통해 접속한 사용자가 업로드 한 파일의 정보를 상기 문서관리 서비스 게이트웨이로 전송하여 상기 문서관리 서비스 게이트웨이가 해당 파일을 암호화하도록 하며, 상기 접속한 사용자의 파일 다운로드 요청할 시에는 해당 요청에 대한 정보를 상기 문서배포 서비스 모듈에 전송하여 상기 문서배포 서비스 모듈이 해당 파일에 대한 암호화된 다운로드 파일을 생성토록 하는 웹서버를 포함하여 구성함을 특징으로 하는 보안 시스템.

【청구항 10】

제9항에 있어서, 상기 사용자 애플리케이션 툴은 초기 설치시와 해당 사용자 시스템의 업그레이드 시에는 상기 사용자 고유 아이디를 생성하며 상기 사용자 정보를 전송함을 특징으로 하는 보안 시스템.

【청구항 11】

제9항에 있어서, 상기 사용자 애플리케이션 툴은 미리 설정된 다수의 문서 편집용 소프트웨어를 호출하여 미리 설정된 윈도우에 출력하여, 사용자로 하여금 상기 문서 편집용 소프트웨어를 실행토록 하는 문서 뷰어 모듈을 구비함을 특징으로 하는 보안 시스템.

【청구항 12】

제11항에 있어서, 상기 문서 뷰어 모듈은 상기 사용자가 상기 문서 편집용 소프트웨어를 상기 윈도우 상에서 수행토록 하며, 상기 문서 편집용 소프트웨어의 실행시에 상기 다운로드 파일의 미리 설정된 규칙 정보 및 해당 사용자 정보에 따라 미리 설정된 파일 저장 및 프린트 동작을 포함하는 미리 설정된 실행제어 동작 수행 여부를 결정함을 특징으로 하는 보안 시스템.

【청구항 13】

제9항에 있어서, 상기 문서키 관리 서비스 모듈, 문서관리 서비스 게이트웨이 및 문서배포 서비스 모듈과 상기 웹서버 간에는 TCP/IP를 이용하여 통신함을 특징으로 하는 보안 시스템.

【청구항 14】

사용자의 시스템 정보를 기반으로 생성된 사용자 고유 아이디를 포함하는 사용자 정보를 관리하는 문서키관리 서비스 모듈과, 업로드된 파일에 대한 문서키를 생성하여 해당 파일을 암호화하여 관리하는 문서관리 서비스 게이트웨이와, 다운로드할 파일의 출력 규칙에 대한 정보를 포함한 암호화된 다운로드 파일을 생성하는 문서배포 서비스 모듈과, 인터넷을 통해 사용자와 파일 업로드/다운로드 동작을 총괄적으로 수행하며 업로드된 파일의 정보를 상기 문서관리 서비스 게이트웨이로 전송하며 다운로드 요청에 대한 정보를 상기 문서배포 서비스 모듈에 전송하는 웹서버를 가지는 디지털 정보 보안 시스템의 디지털 정보 보안 방법에 있어서,

상기 웹서버에서, 파일이 업로드 되는 경우에 상기 파일 업로드에 대한 정보를 상기 문서관리 서비스 게이트웨이에 전송하는 과정과,

상기 문서관리 서비스 게이트웨이에서, 상기 전달받은 파일 업로드에 정보를 이용하여 상기 웹서버의 실제 파일이 업로드 된 위치를 액세스하여 업로된 파일을 액세스하는 과정과,

상기 액세스한 파일에 따른 문서키를 미리 설정된 암호화 방식에 따라 생성하여 해당 파일 정보와 함께 저장하는 과정과,

상기 생성한 문서키를 이용하여 해당 파일을 암호화하는 과정과,

상기 암호화한 파일을 미리 설정된 폴더에 저장하는 과정과,

상기 웹서버로 상기 업로드된 파일에 대한 처리가 완료되었음을 통지하는 과정을 포함하여 이루어짐을 특징으로 하는 보안 방법.

【청구항 15】

제14항에 있어서,

상기 웹서버에서, 상기 접속한 사용자가 파일의 다운로드 요청시에 해당 다운로드 요청된 파일에 대한 정보를 상기 문서배포 서비스 모듈에 전송하는 과정과,

상기 문서배포 서비스 모듈에서, 상기 전달받은 다운로드 요청된 파일 정보를 이용하여 해당 암호화된 파일을 액세스하는 과정과,

상기 해당 접속한 사용자의 사용자 정보와, 상기 해당 문서에 대한 상기 문서키 및 상기 출력 규칙에 대한 정보를 통해 상기 접속한 사용자의 권한에 맞는 암호화된 다운로드 문서 파일을 생성하는 과정과,

상기 생성한 암호화된 다운로드 파일을 다운로드 위치에 저장하는 과정과,

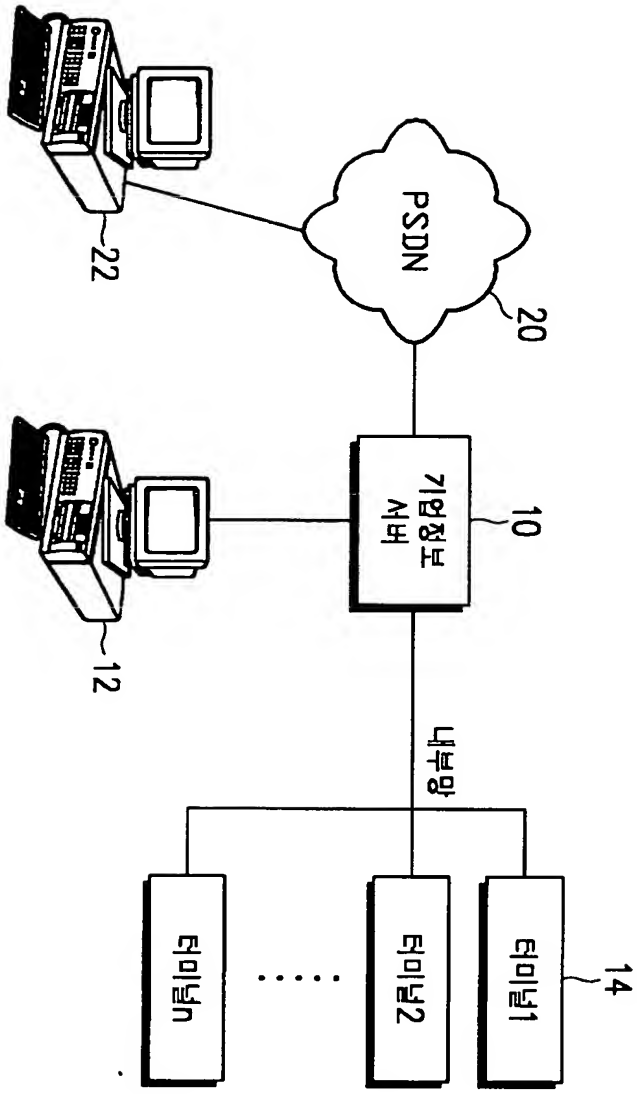
상기 웹서버로 상기 다운로드 요청된 파일에 대한 처리가 완료되었음을 통지하는 과정을 포함하여 이루어짐을 특징으로 하는 보안 방법.

【청구항 16】

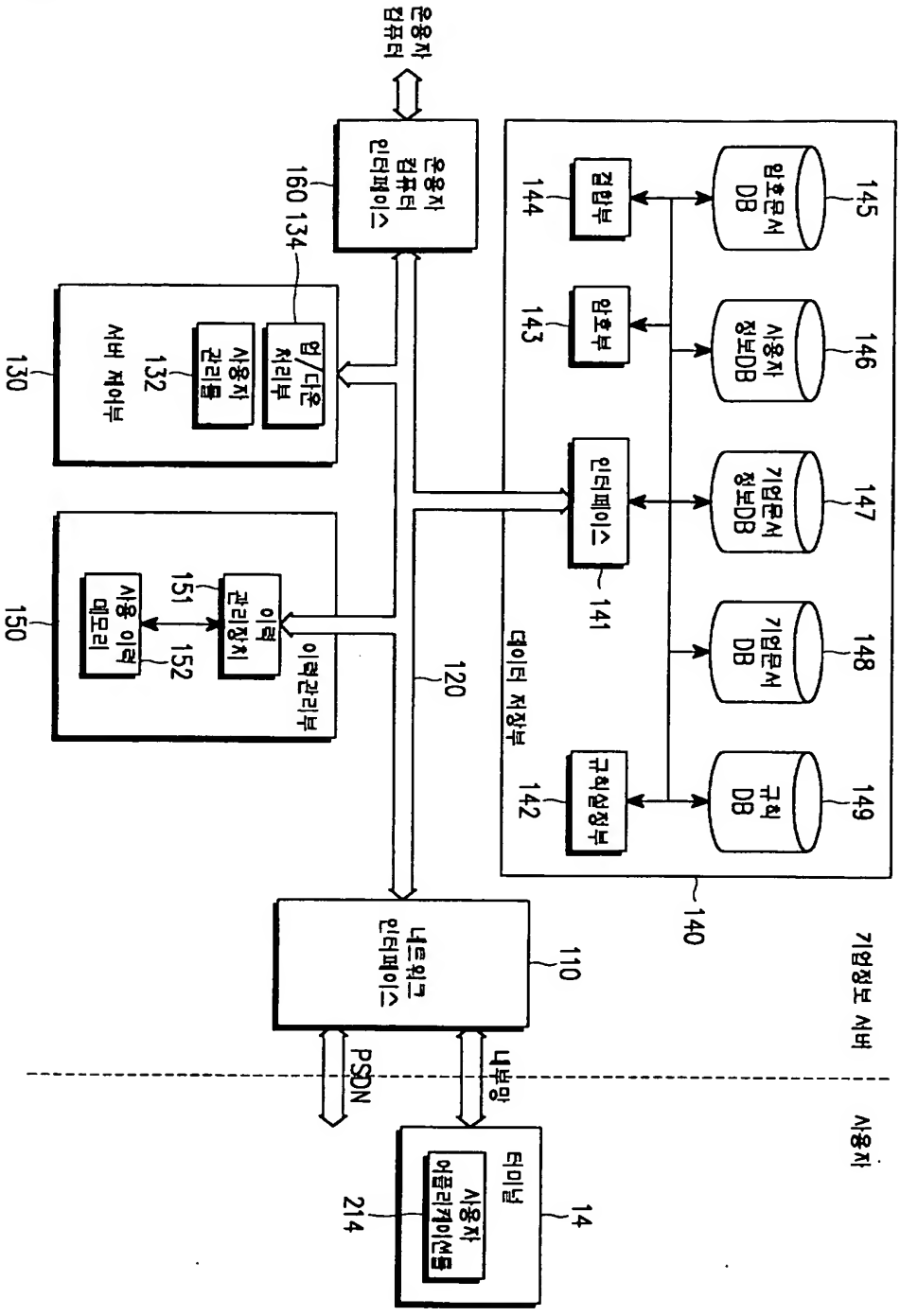
제14항 또는 제15항에 있어서, 상기 출력 규칙에 대한 정보는 상기 접속한 사용자가 상기 다운로드 문서 파일을 자신의 단말기에 저장하는 것의 가능 여부에 대한 규칙인 저장권한과, 상기 다운로드 문서 파일의 프린트 출력 권한 부여 및 횟수에 관한 규칙인 프린트 권한과, 상기 다운로드 문서 파일의 사용 기간에 대한 규칙인 사용기간 권한과, 상기 다운로드 문서 파일의 양도에 관한 규칙인 양도 권한을 포함함을 특징으로 하는 보안 방법.

【도면】

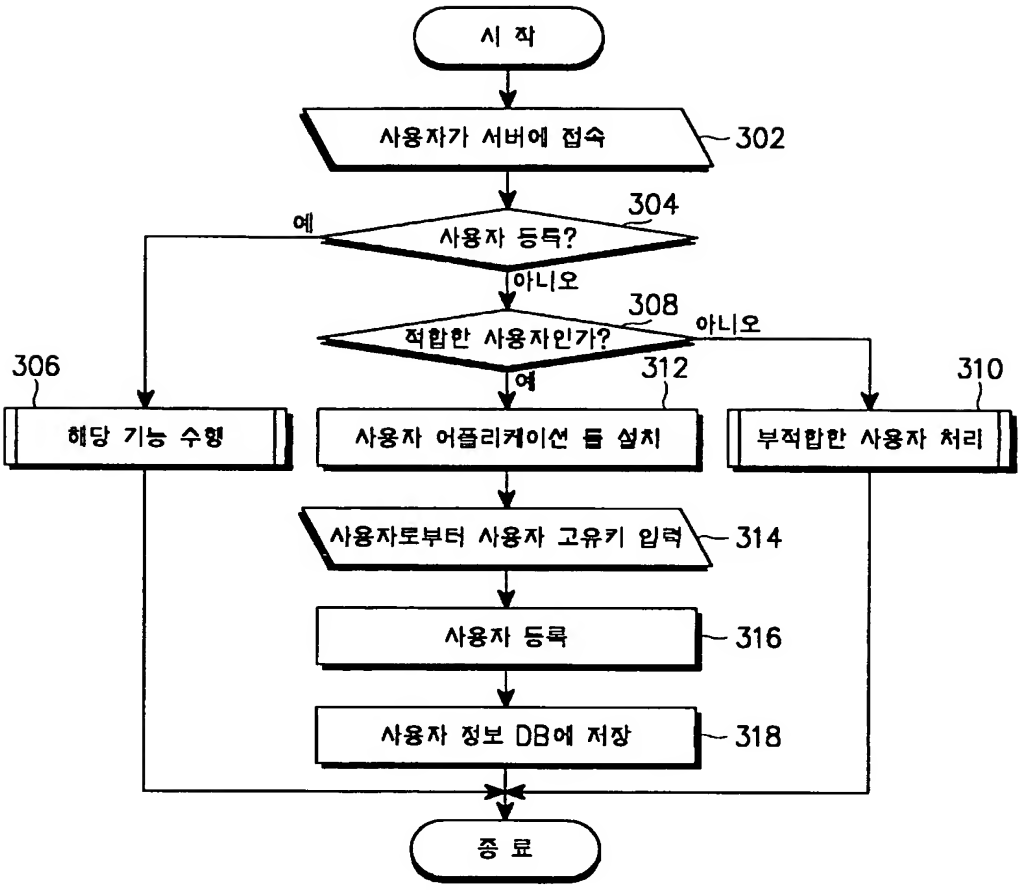
【도 1】



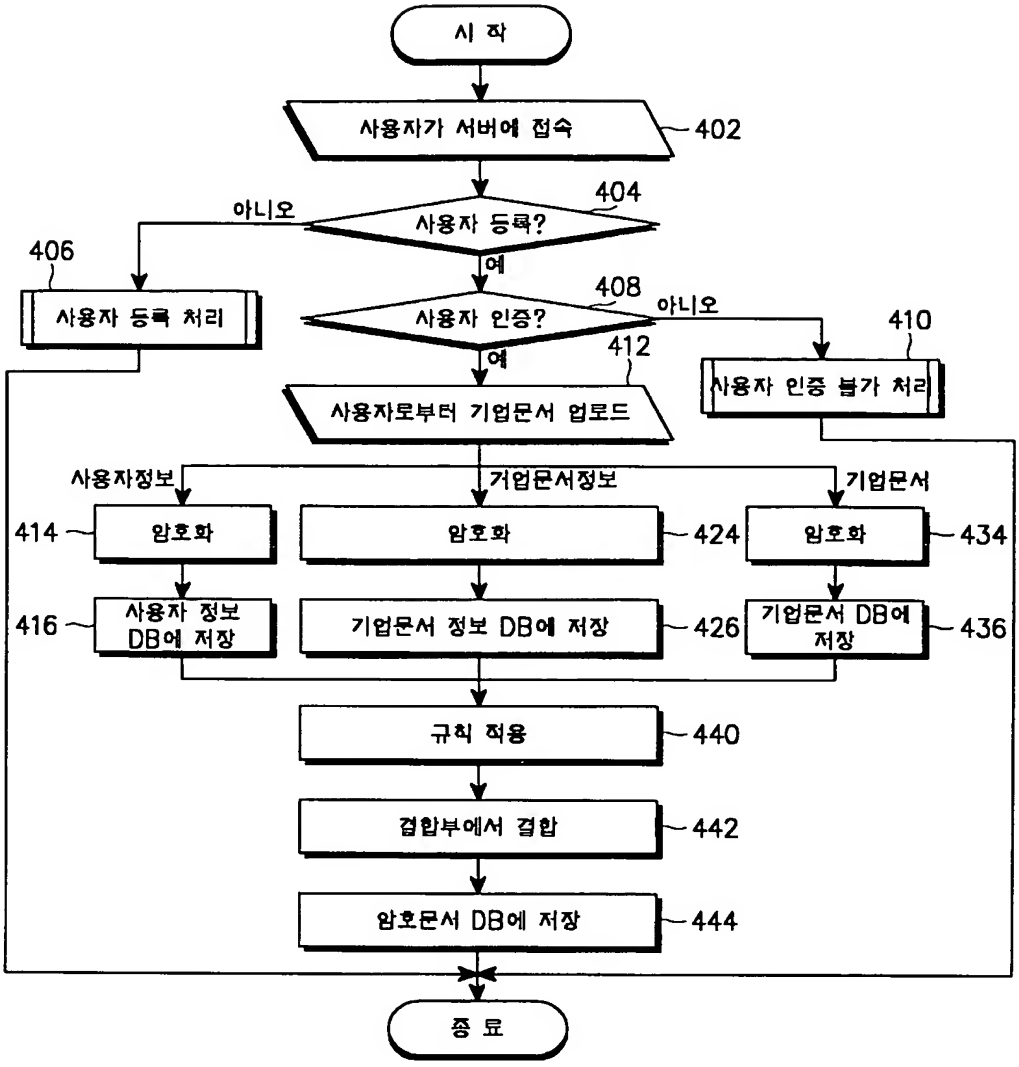
【도 2】


운용자 컴퓨터
운용자 컴퓨터 인터페이스
160
134
업/다운 처리부
사용자 관리부
서버 제어부
130
132
이력 관리장치
사용 이력 메모리
151
152
이력관리부
150
120
인터페이스
141
데이터 저장부
컴파일부
144
암호부
143
규칙설정부
142
암호문서 DB
145
사용자 정보DB
146
기업문서 정보DB
147
기업문서 DB
148
규칙 DB
149
140
기업정보 서버
네트워크 인터페이스
110
PSDN
내부망
사용자
단말기
사용자 어플리케이션들
214
14

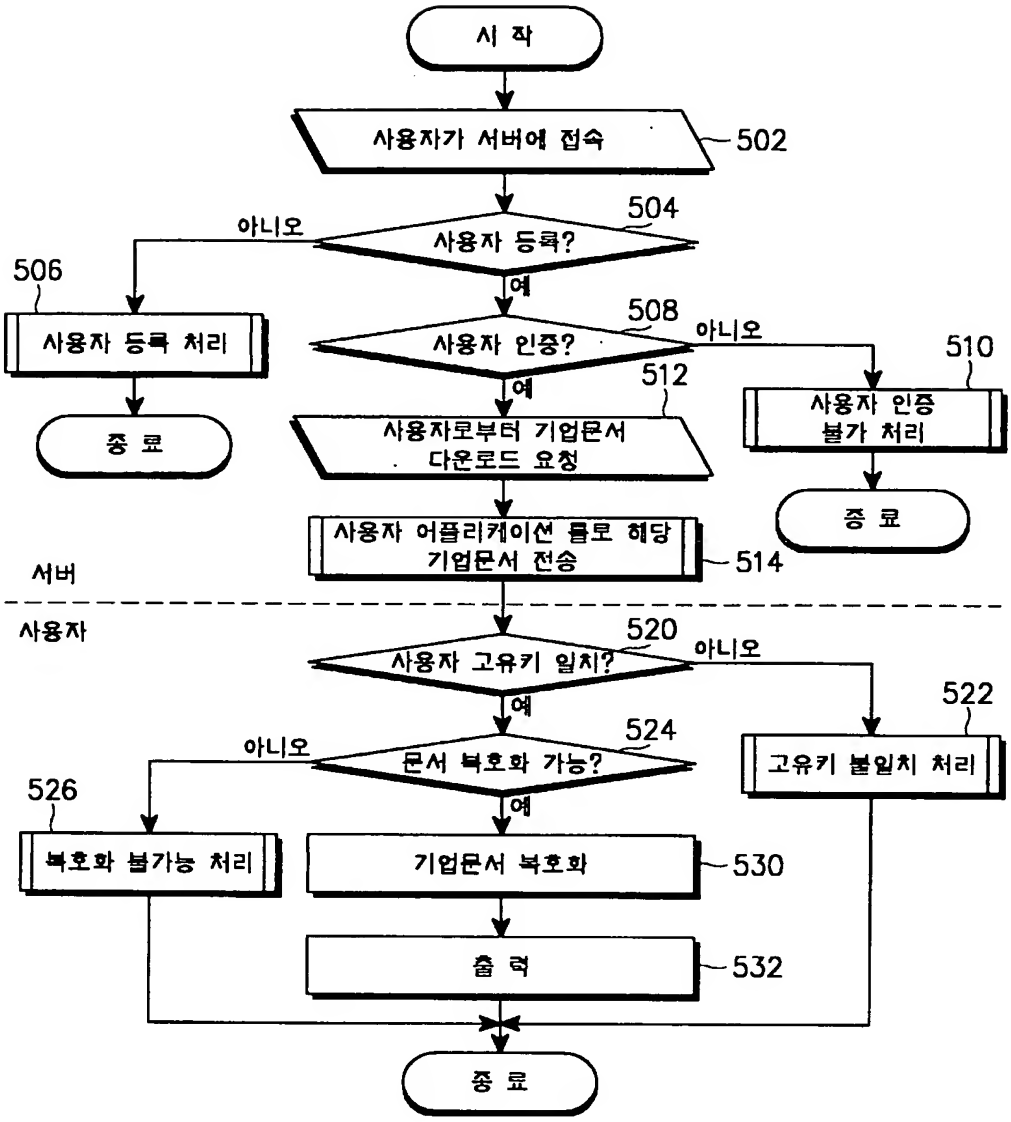
【도 3】


시 작
사용자가 서버에 접속
302
304
사용자 등록?
예
아니오
308
적합한 사용자인가?
아니오
306
312
310
예
해당 기능 수행
사용자 어플리케이션 등 설치
부적합한 사용자 처리
사용자로부터 사용자 고유키 입력
314
사용자 등록
316
사용자 정보 DB에 저장
318
종 료

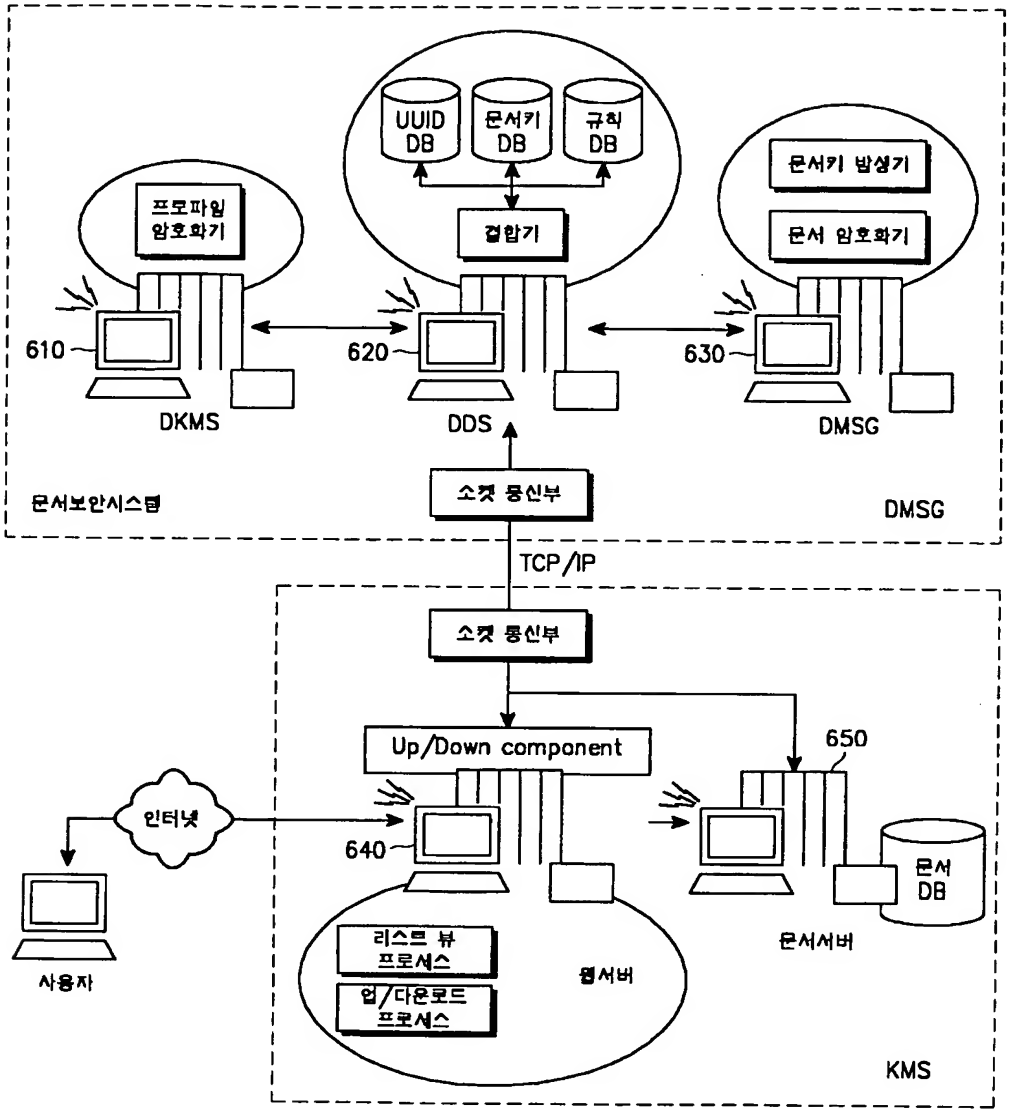
【도 4】


시 작
사용자가 서버에 접속
402
사용자 등록?
404
아니오
예
406
사용자 등록 처리
사용자 인증?
408
아니오
예
410
사용자 인증 불가 처리
412
사용자로부터 기업문서 업로드
사용자정보
거업문서정보
기업문서
414
암호화
424
암호화
434
암호화
416
사용자 정보 DB에 저장
기업문서 정보 DB에 저장
426
기업문서 DB에 저장
436
규칙 적용
440
결합부에서 결합
442
암호문서 DB에 저장
444
종 료

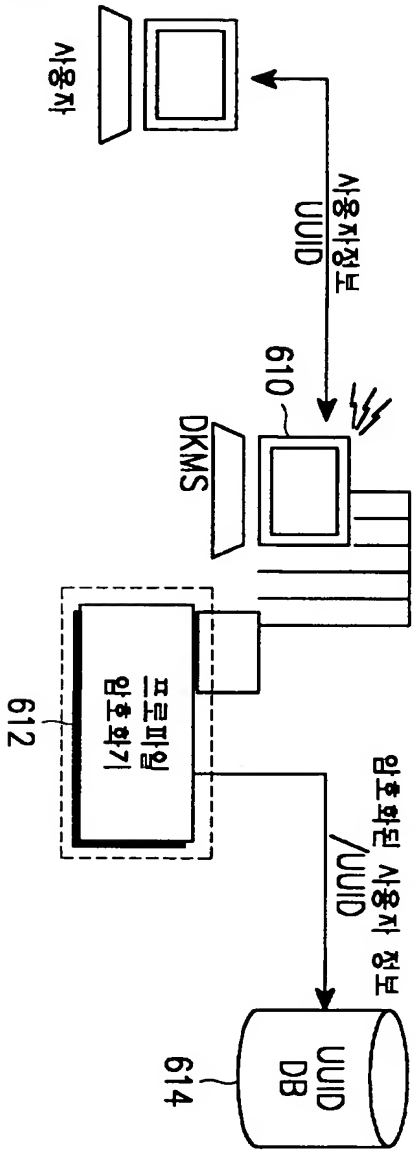
【도 5】


시 작
사용자가 서버에 접속
502
사용자 등록?
504
아니오
여
506
사용자 등록 처리
종 료
사용자 인증?
508
아니오
여
510
사용자 인증 불가 처리
종 료
512
사용자로부터 기업문서 다운로드 요청
사용자 어플리케이션 툴로 해당 기업문서 전송
514
서버
사용자
사용자 고유키 일치?
520
아니오
여
522
고유키 불일치 처리
문서 복호화 가능?
524
아니오
여
526
복호화 불가능 처리
기업문서 복호화
530
출 력
532
종 료

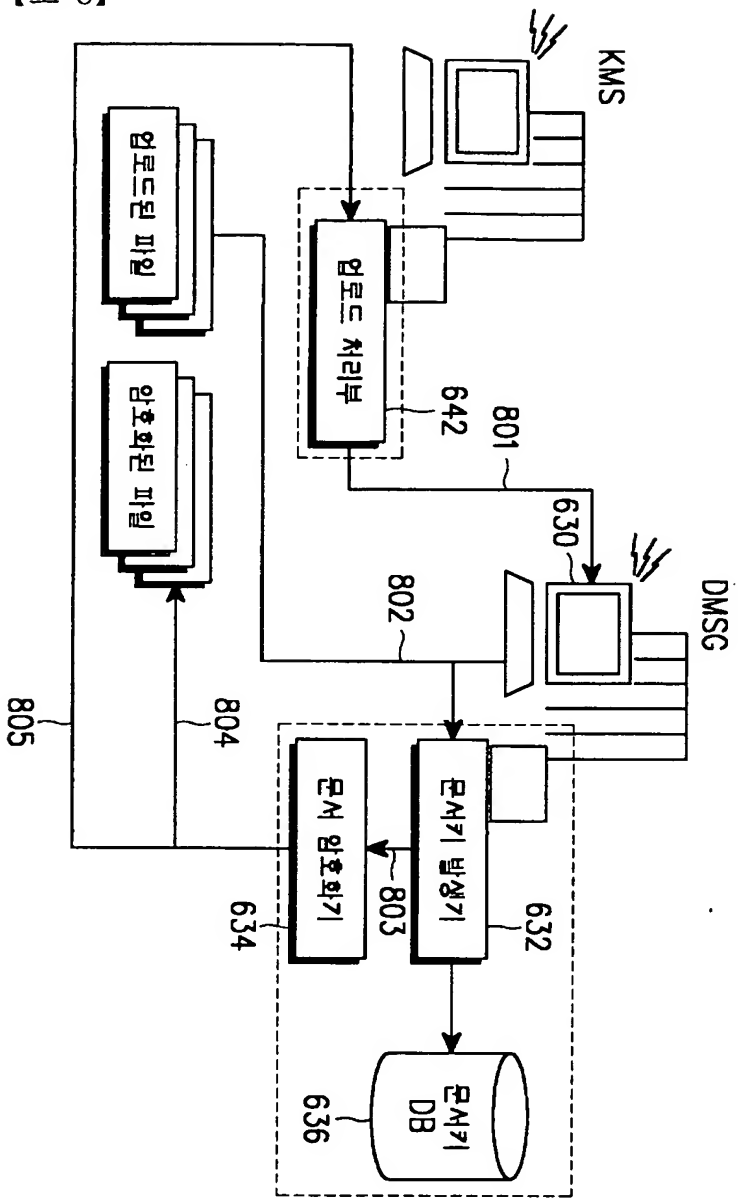
【도 6】


UUID DB
문서키 DB
규칙 DB
결합기
프로파일 암호화기
문서키 발생기
문서 암호화기
610
620
630
DKMS
DDS
DMSG
문서보안시스템
소켓 통신부
DMSG
TCP/IP
소켓 통신부
Up/Down component
650
인터넷
640
문서 DB
리스트 뷰 프로세스
업/다운로드 프로세스
웹서버
문서서버
사용자
KMS

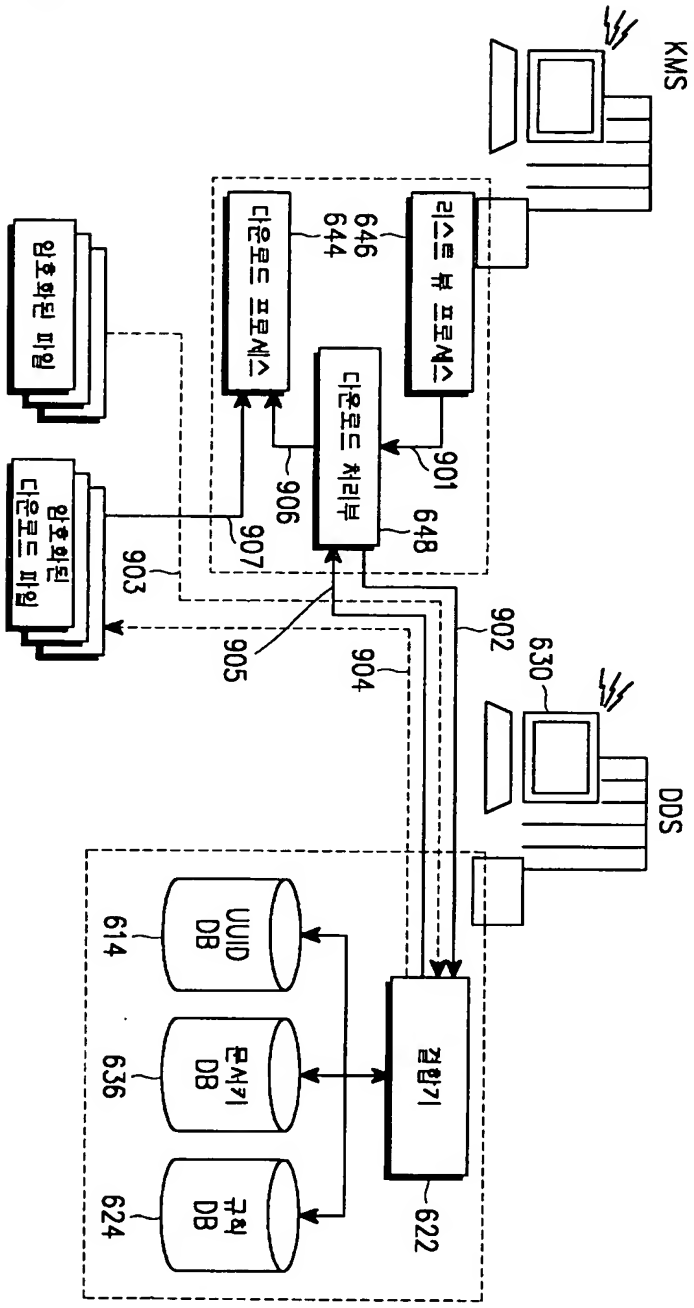
【도 7】


사용자
사용자정보 UUID
610
DKMS
612
프로파일 암호화기
암호화된 사용자 정보 UUID
614
UUID DB

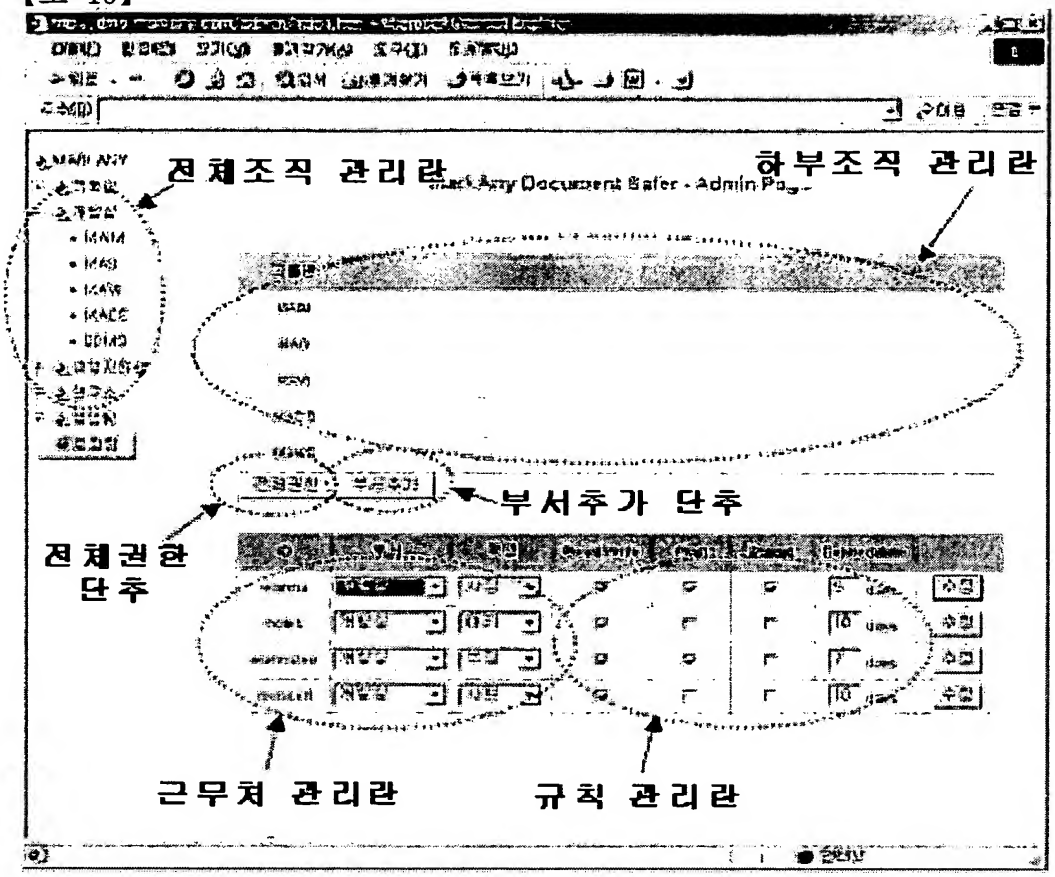
【도 8】


KMS
업로드 컨텐츠 파일
암호화된 컨텐츠 파일
업로드 처리부
642
801
630
DMSG
802
805
804
문서 암호화기
문서키 발생기
803
634
632
문서키 DB
636

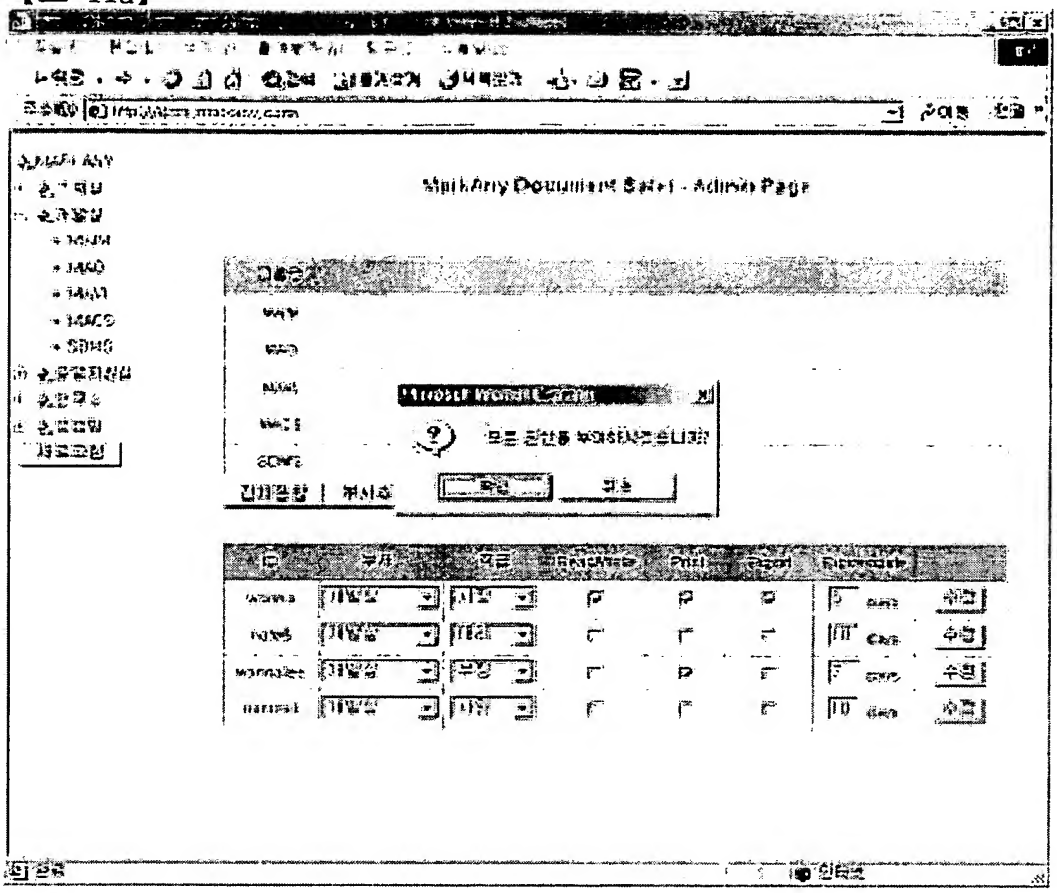
【도 9】


KMS
다운로드 프로세스
646
644
리스트 뷰 프로세스
암호화된 파일
다운로드 처리부
901
906
907
648
암호화된 다운로드 파일
903
905
904
902
630
DDS
UUID DB
614
문서키 DB
636
결합기
규칙 DB
624
622

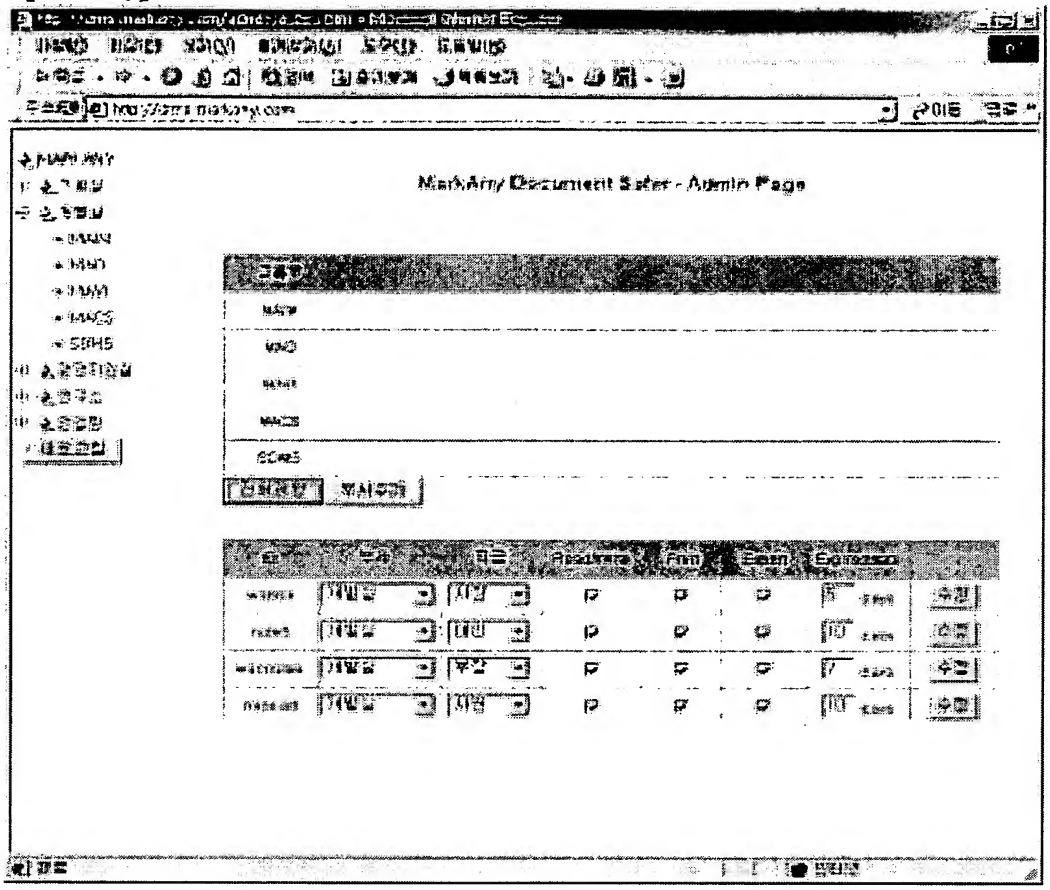
【도 10】



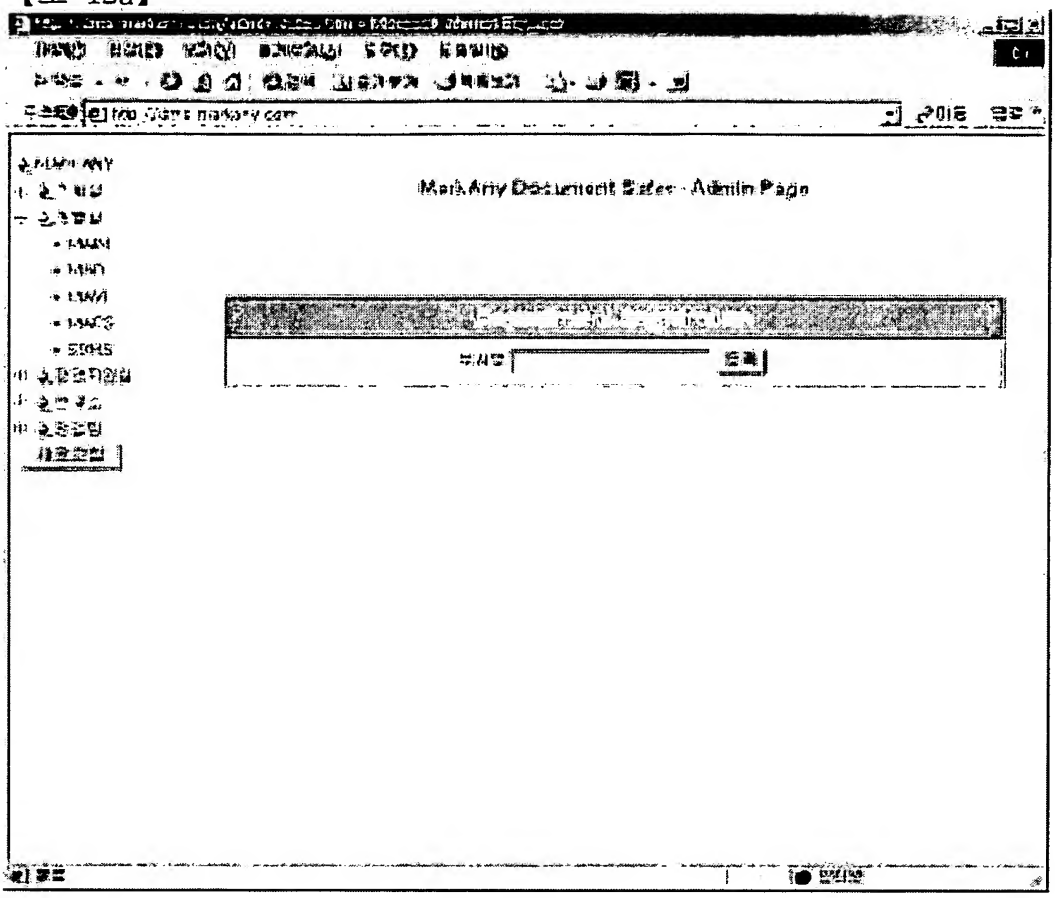
【도 11a】



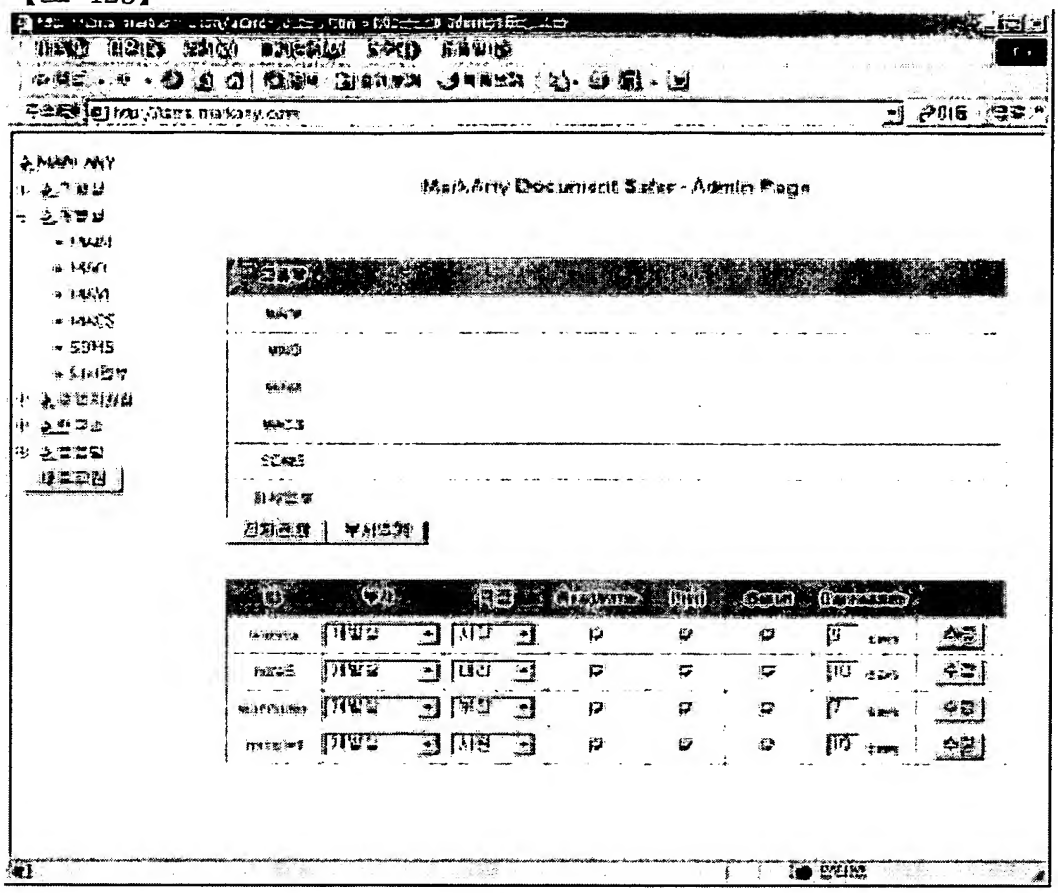
【도 11b】



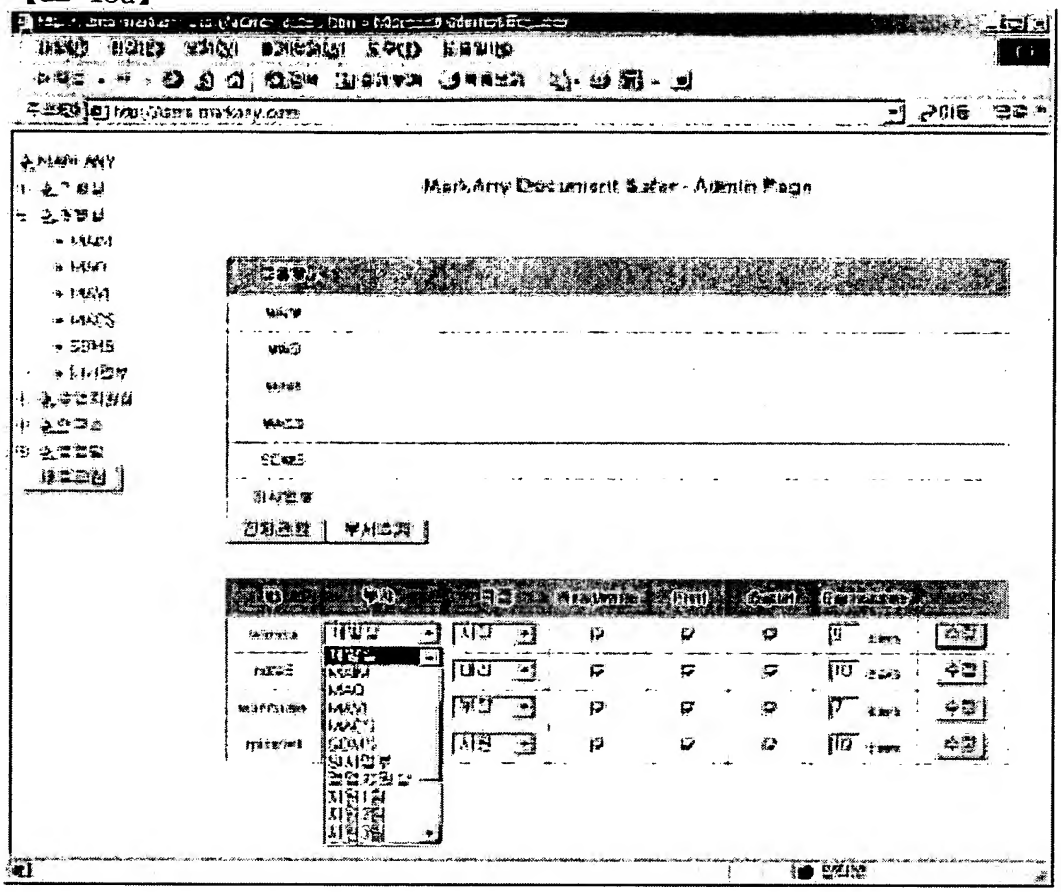
【도 12a】



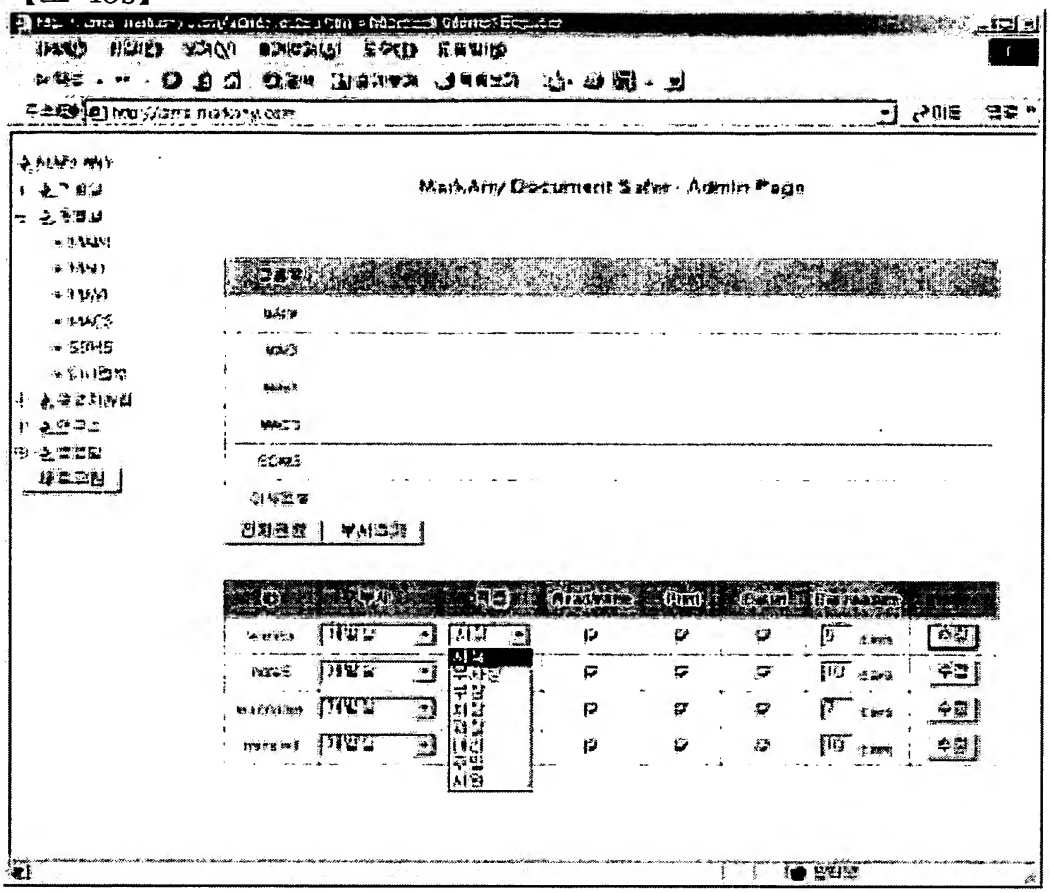
【도 12b】



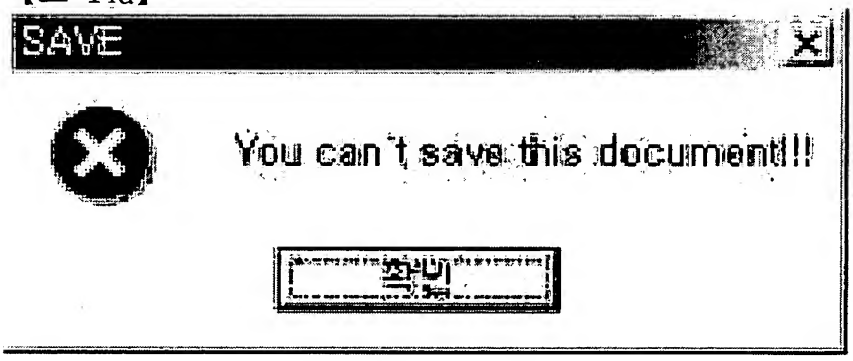
【도 13a】



【도 13b】

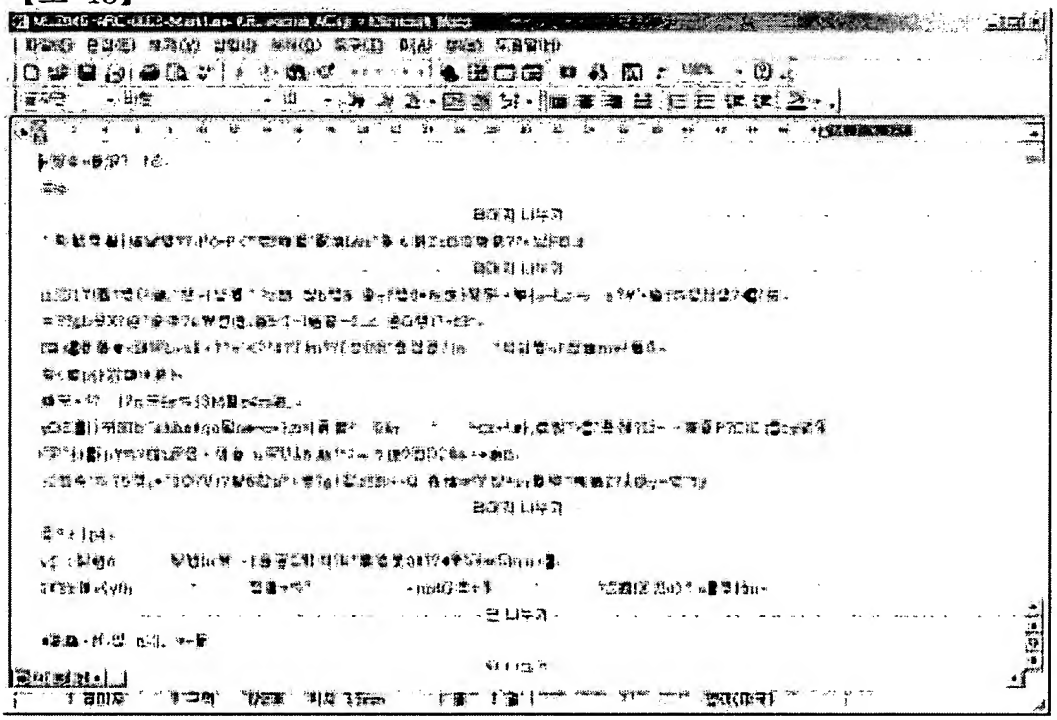

Main Army Document Saver - Admin Page

【도 14a】

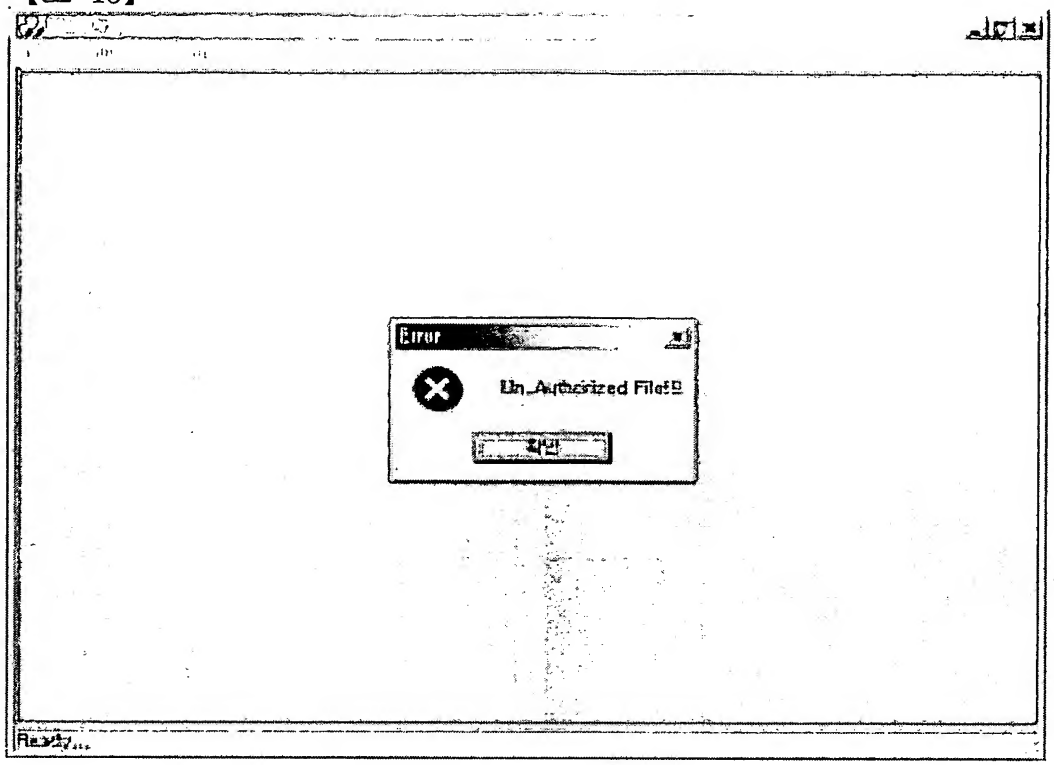

SAVE
You can't save this document!!

【도 14b】

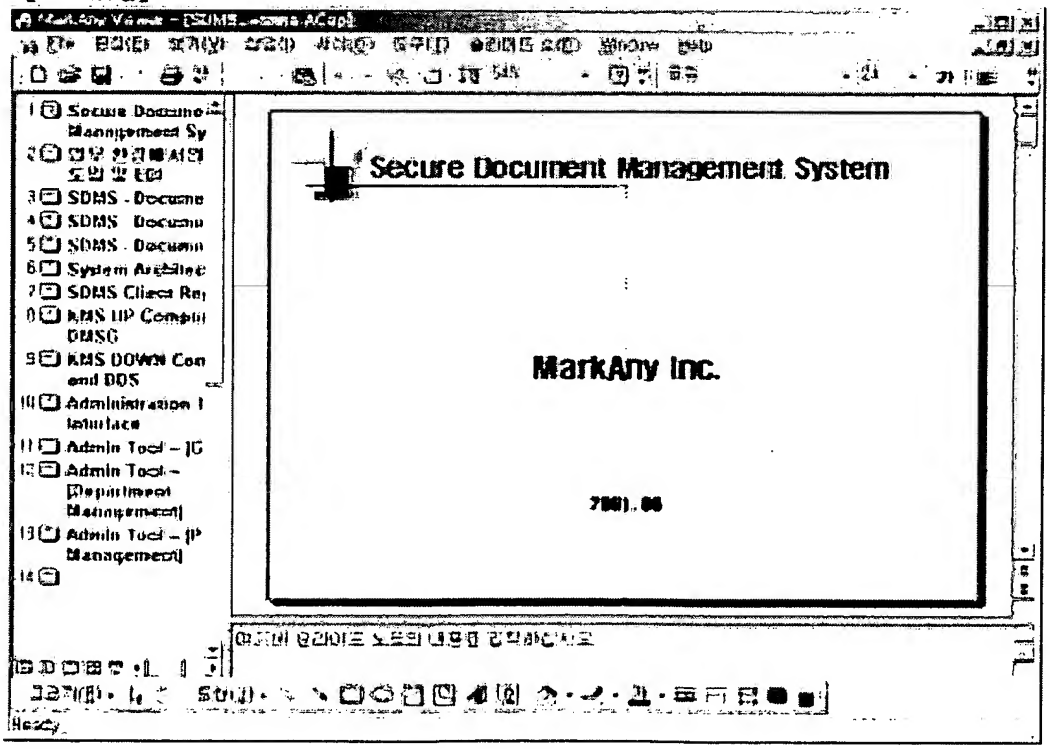
【도 15】



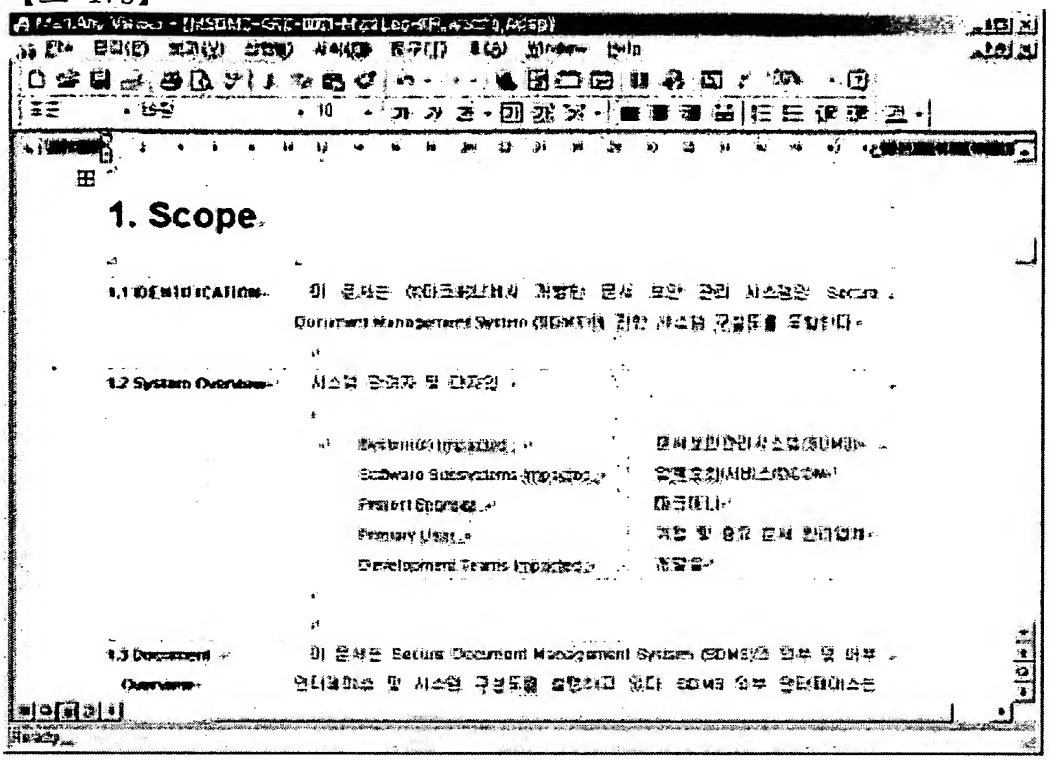
【도 16】


Error
Un_Authorized File!!
확인
Ready...

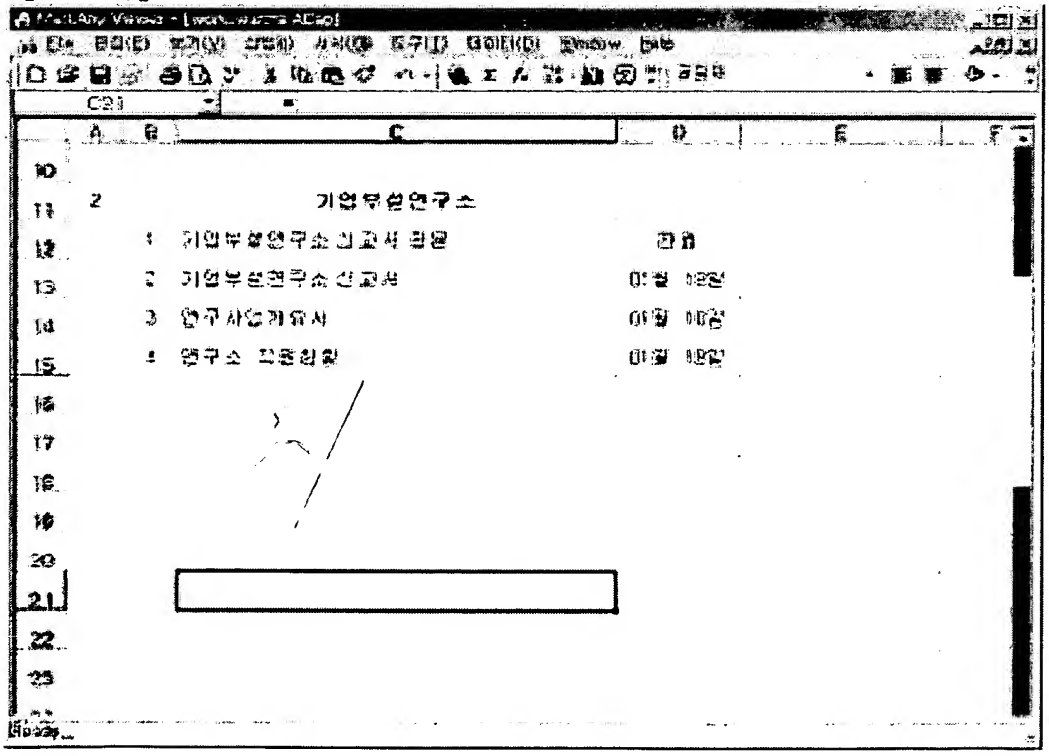
【도 17a】


Secure Document Management System
MarkAny Inc.
Ready

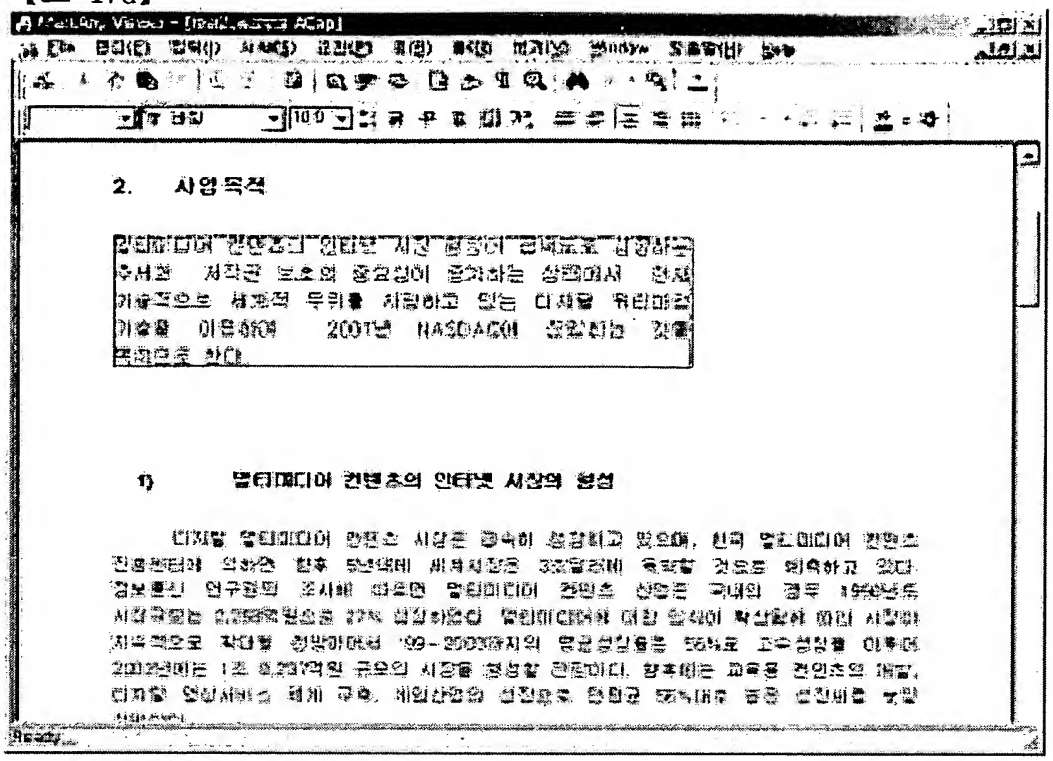
【도 17b】



【도 17c】



【도 17d】



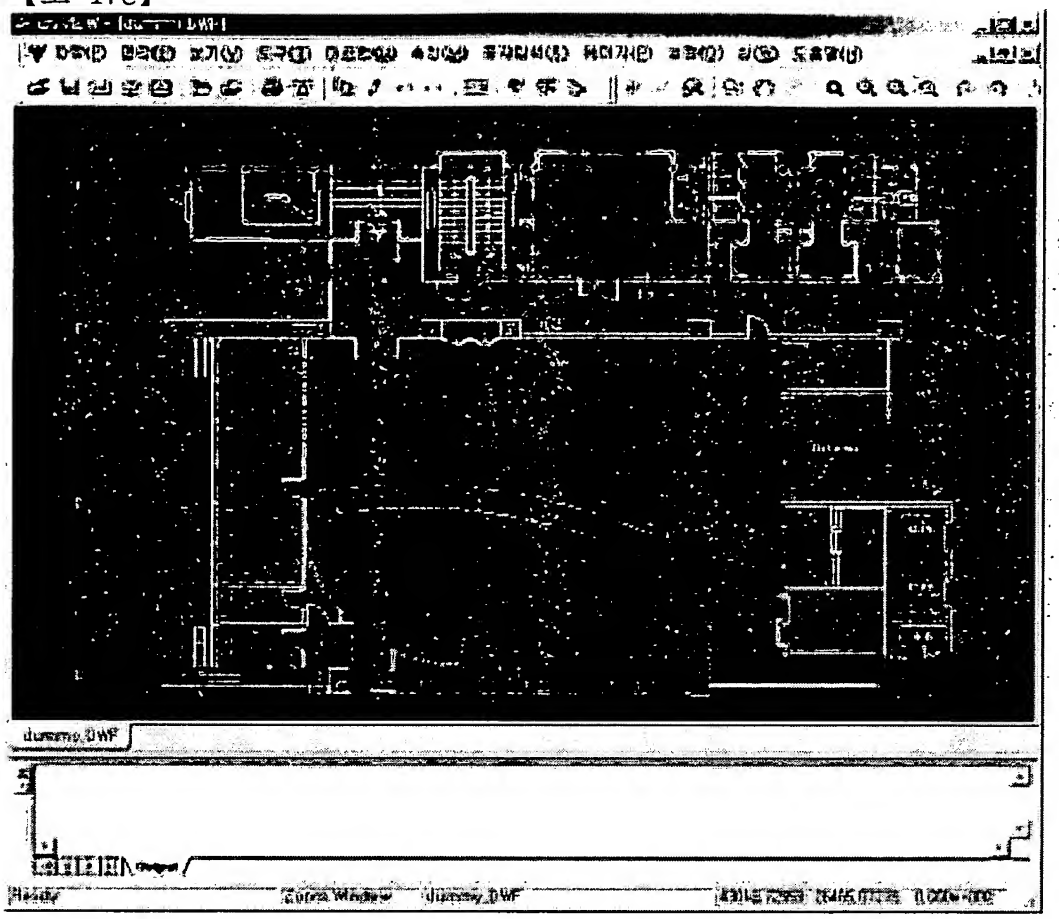
2. 사업목적

[redacted]

1) 멀티미디어 컨텐츠의 인터넷 시장의 분석

[redacted]

【도 17e】



【서지사항】

【서류명】	서지사항 보정서
【수신처】	특허청장
【제출일자】	2001.08.14
【출원인】	
【명칭】	주식회사 마크애니
【출원인코드】	1-1999-026375-7
【사건과의 관계】	출원인
【대리인】	
【성명】	권혁록
【대리인코드】	9-1998-000115-1
【사건의 표시】	
【출원번호】	10-2001-0045856
【출원일자】	2001.07.30
【발명의 명칭】	디지털 정보 보안 방법 및 그 시스템
【제출원인】	
【발송번호】	1-5-2001-0037866-87
【발송일자】	2001.08.08
【보정할 서류】	특허출원서
【보정할 사항】	
【보정대상 항목】	첨부서류
【보정방법】	제출
【보정내용】	
【첨부서류】	1. 중소기업법시행령 제2조에의한 중소기업에 해당함을 증명 하는 서류_1통 2.위임장_1통
【취지】	특허법시행규칙 제13조·실용신안법시행규칙 제8조의 규정에의하여 위와 같 이 제출합니다. 대리인 권혁록 .(인)
【수수료】	
【보정료】	11,000 원
【기타 수수료】	0 원
【합계】	11,000 원
【첨부서류】	1. 기타첨부서류_1통[중소기업법시행령 제2조에 의한 중소기업에 해당 함을 증명하는 서류] 2.위임장_1통